UNIVERSIDADE DE LISBOA
FACULDADE DE DIREITO

A OPERAÇÃO BANCÁRIA ABERTA

MESTRADO EM DIREITO E PRÁTICA JURÍDICA
ESPECIALIDADE DE DIREITO DA EMPRESA

LEONOR XIMENES DE MESQUITA

PROFESSOR(A) ORIENTADOR(A)
ANA PERESTRELO DE OLIVEIRA

LISBOA, 2020

AGRADECIMENTOS

Com a realização da minha Dissertação de Mestrado termino um percurso académico muito intenso e desafiante. Hoje com uma Licenciatura em Direito, um programa Erasmus com a duração de um ano em Berlim e um Mestrado em fase de conclusão, posso afirmar convictamente que foi o melhor percurso que podia ter escolhido. Não o conseguiria ter alcançado sem o contributo das pessoas que me acompanharam durante esse percurso e a quem não posso deixar de expressar os meus agradecimentos:

Aos meus pais, por tudo o que me proporcionaram a mim e aos meus irmãos, pelo carinho, pelo apoio incondicional, pela educação, e por todos os sacrifícios que fizeram em benefício do meu percurso académico.

Aos meus quatro irmãos, pela companhia e pelas histórias que partilhamos.

Ao Diogo, uma pessoa muito especial que nunca me deixou desistir e que acredita sempre em mim.

À minha querida sobrinha Maria da Luz, que embora apenas tenha um mês e meio de idade já é uma pessoa tão importante na minha vida.

Aos meus amigos de sempre, pela amizade e por tornarem a minha vida mais divertida e descontraída.

À Professora Doutora Ana Perestrelo de Oliveira, pela partilha de conhecimentos e pela orientação disponibilizada durante este percurso.

A Operação Bancária Aberta

RESUMO

Nas últimas décadas, a interseção entre novas tecnologias e serviços de pagamento possibilitaram uma profunda mudança nos hábitos de pagamento e no paradigma das relações bancárias tradicionais. Fruto da digitalização dos serviços de pagamento foi a consagração de uma nova categoria de atores no mercado que apresentou serviços de pagamento baseados em soluções tecnológicas e passou a prestar serviços mais céleres, pouco onerosos e cómodos.

A entrada em vigor da Segunda Diretiva de Serviços de Pagamento deu origem ao reconhecimento da existência e importância dos novos serviços de pagamento no mercado – o serviço de iniciação de pagamentos e o de informação sobre contas. O reconhecimento permitiu "abrir" o mercado, que até então pertencia primordialmente às instituições de crédito. O aparecimento de novos intervenientes provocou uma necessidade de alterar o ultrapassado modelo de negócio baseado na intermediação financeira, substituindo este por serviços de pagamento por meios digitais, inovadores, seguros e de fácil utilização. A partilha da quota de mercado alavancou, por sua vez, o surgimento de um clima de concorrência e eficiência dos agentes económicos.

O fenómeno da "abertura" das instituições de crédito denomina-se *Operação Bancária Aberta*. No presente trabalho propomo-nos a aprofundar este instituto, o seu surgimento, a legislação aplicável, em que medida opera a operação de recolha, tratamento, agregação e disponibilização da informação bancária, os deveres que incumbem a cada uma das partes e ainda a determinação da responsabilidade no âmbito da partilha de dados.

PALAVRAS-CHAVE: OPERAÇÃO BANCÁRIA ABERTA, DADOS BANCÁRIOS, PARTILHA DE DADOS

ABSTRACT

In the last few decades, the intersection between new technologies and payment services has enabled a deep change in the payment habits and the paradigm of traditional banking relationships. The result of the digitalization of payment services has been the consecration of a new category of players in the market who have presented payment services based on technological solutions and started to provide faster, lower cost and more convenient services.

The entry into force of the Second Payment Services Directive gave rise to recognition of the existence and importance of the new payment services in the market - the payment initiation service and the account information service. This recognition allowed "opening" the market, which until then belonged primarily to credit institutions. The emergence of new players caused a need to change the outdated business model based on financial intermediation, replacing it with payment services by digital, innovative, secure and user-friendly means. The sharing of market share has, in turn, leveraged the emergence of an environment of competition and efficiency of the different economic agents.

The phenomenon of "opening" of credit institutions is called Open Banking. In the present work we propose to deepen this institution, its emergence, the applicable legislation, the extent to which it operates the operation of collection, processing, aggregation and availability of banking information, the duties incumbent on each of the parties and also the determination of responsibility in the area of data sharing.

KEYWORDS: OPEN BANKING, BANK DATA, DATA SHARING

LISTA DE ABREVIATURAS

Ac.	Acórdão
Art.	Artigo
CC	Código Civil
CE	Comissão Europeia
Cfr.	Confrontar
DSP 1	Primeira Diretiva dos Serviços de Pagamento 2007/64/CE
DSP 2	Segunda Diretiva dos Serviços de Pagamento 2015/2366
EU	European Union
Ed.	Edição
n.º	Número
p.	Página
pp.	Páginas
Proc.	Processo
RGICSF	Regime Geral das Instituições de Crédito e Sociedades Financeiras
RJSPME	Regime Geral dos Serviços de Pagamento e Moeda Eletrónica
RGPD	Regulamento Geral sobre a Proteção de Dados
STJ	Supremo Tribunal de Justiça
Vol.	Volume

1) INTRODUÇÃO

A interseção entre a tecnologia e os serviços financeiros não é um fenómeno recente. Desde os serviços de multibanco, ao cartão de crédito e de débito até aos pagamentos *online* são tudo mecanismos que a tecnologia aplicada aos serviços financeiros foi atingindo. Vários fatores têm contribuído para esta nova realidade – o acesso cada vez mais generalizado e facilitado à *Internet*, a evolução do comércio eletrónico, os hábitos dos consumidores, entre outros.

Nas últimas décadas assistimos a uma acelerada evolução tecnológica, que provocou uma digitalização dos serviços mais tradicionais do mercado financeiro. O paradigma das relações bancárias, como conhecido até recentemente, tem sofrido muitas alterações e tem sido alvo de uma inovação crescente nos últimos anos.

Os modelos de negócio tradicionais e baseados na intermediação financeira têm vindo a perder força nesta nova realidade mais digital. Começando pela referência à emissão de cartões de crédito e de débito, que permitiram a realização de operações de pagamento, depósito, ou até, transferência, tudo através de um terminal ou do recurso a uma caixa multibanco. Mais recentemente o surgimento do serviço de *home banking* que permite a realização de uma multiplicidade de operações bancárias, à distância, com recurso apenas a um instrumento disponibilizado pelo banco através da internet.

Esta disrupção tecnológica no mercado financeiro não parou aqui. O surgimento destes novos serviços foi apenas o início e veio, acima de tudo, abrir caminho para novos tipos de serviços e de prestadores.

A tecnologia avançada, aplicada a serviços financeiros, permitiu substituir a relação distante e formal existente entre o cliente e o banco. Esta substituição foi, em grande parte, impulsionada pelo aparecimento de novas e inovadoras entidades, prestadoras de serviços de pagamento, que para a disponibilização dos mesmo serviços financeiros faziam recuso à tecnologia.

As *Fintech*[1], denominação que decorre da conjugação de duas palavras inglesas, *Financial* e *Technology*, permitiu prescindir do fator físico ou presencial, aquando da

[1] Sobre *Fintech, vide* CARLOS MOURA, "*FinTech e regulação no mercado bancário*", in *FinTech* - Desafios da Tecnologia Financeira, Vol. 2, 1ª ed., Almedina, 2019, p. 21

celebração de contratos ou da realização de operações. Hoje em dia é possível realizar qualquer operação bancária de modo rápido, cómodo e gratuito recorrendo aos mesmos serviços apenas através da *internet*.

É neste contexto e em sintonia com a inovação tecnológica que surge a Operação Bancária Aberta[2]. A Operação Bancária Aberta é um modelo colaborativo entre duas ou mais entidades, que opera através da partilha de dados bancários, com recurso a interfaces de programação de aplicação.

Ao longo dos últimos anos registou-se uma mudança significativa nos hábitos de pagamento em Portugal: os instrumentos de pagamento eletrónicos ganharam importância (cartões, débitos diretos e transferências a crédito) e os cheques, pelo contrário, conheceram uma redução significativa. Apesar de Portugal registar uma das mais baixas taxas de utilizadores de comércio eletrónico da zona euro[3], o aumento do recurso a instrumentos de pagamento eletrónico [4]. O alargamento do comércio eletrónico, aliado à crescente facilidade de acesso da população à internet[5], possibilitou o

[2] Do inglês, "*Open Banking*"

[3] Autoridade da Concorrência, *Inovação Tecnológica e Concorrência no Setor Financeiro em Portugal*, Issues Paper, 2018, com base em dados da Eurostat: *Individuals using the internet for ordering goods or services e Individuals who have basic or above basic overall digital skills by sex*, disponíveis em: http://ec.europa.eu/eurostat/web/products-datasets/product?code=tin00096: As aquisições de bens e serviços através da internet são um dos contextos de mercado particularmente propícios à proliferação de novos serviços de pagamento, nomeadamente os associados à FinTech. Contudo, as compras online e por dispositivo móvel, em Portugal, assumem uma expressão ainda reduzida face a outros países da zona euro. Com efeito, o comércio online representava, em 2017, cerca de 3,9% do volume e 5,9% do valor de compras efetuadas por cartão, de acordo com dados do Banco de Portugal. Em 2017, 34% dos indivíduos com idades compreendidas entre os 16 e os 74 anos utilizaram a internet para comprar bens e serviços, sendo este valor de 57% para a zona euro. Esta discrepância só é, em parte, explicada por diferenças nas competências digitais, já que 50% da mesma amostra tinha pelo menos competências digitais básicas, sendo este valor de 58% para a zona euro.

[4] Disponível em https://www.bportugal.pt/page/instrumentos-de-pagamento?fbclid=IwAR3RsViVd4298NBYJ1Yo971921NLFPb8R1gJu_9KKrp7_sBPD-beOcIdmkA

[5] O Banco de Portugal publicou o Relatório dos Sistemas de Pagamento, por referência ao ano de 2019, nos termos do qual comunica que o sistema, que abrange os pagamentos de retalho em Portugal, processou 3 mil milhões de operações, no valor de 523,1 mil milhões de euros, o que representa, em média, 8,7 milhões de operações por dia, no valor de 1,9 mil milhões de euros. O crescimento foi de 9,3% em número, a maior taxa nos últimos cinco anos, e mais 6,4% em valor do que em 2018. Este aumento continuou a ser sustentado pelos instrumentos de pagamento eletrónicos (débitos diretos, transferências a crédito, transferências imediatas e operações de pagamento baseadas em cartão), que representaram 99,1% do número e 83,9% do valor total do SICOI. Acrescenta que em 2019, os consumidores começaram a utilizar de forma significativa os pagamentos *contactless*. Este comportamento terá resultado, entre outros fatores, dos aumentos do número de cartões e de terminais com esta tecnologia, de 27,5% e 20,7%, respetivamente. As

aparecimento de serviços financeiros inovadores. Contudo, se a digitalização de um dos setores mais tradicionalistas trouxe muitas vantagens, sendo um ramo recente e atual, também dá aso a situações desvantajosas.

No contexto da operação bancária aberta, a partilha de dados pessoais do utilizador do serviço é um elemento chave do processo. A entidade prestadora do serviço terá de ter tido acesso à informação detida (até agora) pelo banco. O cliente, titular dos dados aos quais nos referimos, detidos pelo banco, goza de uma proteção conferida pelo contrato de abertura de conta, celebrado com o banco. O banco vê-se obrigado a disponibilizar os dados dos seus clientes a uma entidade terceira à relação contratual que tem com o seu cliente.

O valor que os dados pessoais têm vindo a ganhar, nos últimos anos, faz sentir-se no âmbito da operação bancária aberta. Associado a esta partilha de dados está o risco de perda, extravio ou adulteração da informação prestada.

O processo associado à operação bancária aberta pressupõe a intervenção de três sujeitos – o utilizador/cliente; o banco e a entidade prestadora do serviço. Para que o processo esteja concluído, todos os intervenientes têm deveres e obrigações a que estão adstritos. Nesta dissertação procuraremos analisar de um ponto de vista jurídico o instituto da operação bancária aberta.

Num primeiro momento, apresentamos o conceito da operação bancária aberta e o seu surgimento no mercado único. Neste âmbito analisaremos, igualmente, o quadro legislativo dos serviços de pagamento, que serve de base legal para a regulação deste serviço. Essencialmente focaremos a nossa análise na Segunda Diretiva Europeia de Serviços de Pagamento, sendo este o primeiro diploma que prevê e reconhece este novo tipo de serviço de pagamento. Neste contexto, não podemos deixar de colocar especial

---

compras com recurso à tecnologia *contactless* representaram 7,8% do número e 3% do valor total de compras com cartão, duplicando assim o seu peso face ao total das compras em comparação com 2018. Cada compra com *contactless* teve um valor médio de 14,5 euros e os principais setores em que esta tecnologia foi utilizada foram o comércio a retalho e a restauração.
As compras *online* com cartões nacionais também cresceram: 43% em número e 28% em valor, representando, respetivamente, 6,3% e 7,5% do número e do valor das compras realizadas com cartões emitidos em Portugal. A maioria das compras *online* (80% do número e do valor) foram efetuadas a comerciantes no estrangeiro. Dados disponíveis em https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/rsp2019_0.pdf

foco na estrutura contratual entre as partes intervenientes e nos deveres a que lhes incumbe.

Num segundo momento focar-nos-emos na questão dos dados pessoais do utilizador/cliente bancário. Em especial, cumpre enquadrar os dados bancários enquanto dados pessoais recorrendo para tal à análise do Regulamento n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

Por fim, procuraremos explorar a questão da responsabilidade por danos decorrente do recurso à operação bancária. Em especial procuraremos focar-nos no tema da repartição de responsabilidade e dos prejuízos[6], i.e., da imputação de responsabilidade aos intervenientes do processo, por operações não autorizadas e/ ou danos provocados, no seguimento da utilização de serviço operação bancária aberta.

Tomamos dois temas como essenciais na resolução de um litígio neste âmbito – a imputação da responsabilidade por operações bancárias não autorizadas e o ónus da prova do banco, por um lado, e do novo prestador do serviço de pagamento por outro.

Para tal, consideramos prudente proceder a uma análise do regime geral da responsabilidade civil do Código Civil ("CC") Português, bem como do regime apresentado pelo Decreto-Lei n.º 91/2018, de 12 de novembro, que aprova o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica e, ainda, a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno. Ao longo desta análise não deixaremos de fazer referência às decisões que ultimamente têm vindo a ser proferidas pelos Tribunais.

[6] Sobre este tema têm os Tribunais dado especial enfoque, tendo a primeira sentença sobre o tema sido proferida pelo Tribunal da Relação de Lisboa, de 26/10/2020, com o relator Maria Amélia Ribeiro, disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/20a5cc803440273e802577ed003c0299?OpenDocument

2) DA OPERAÇÃO BANCÁRIA ABERTA

2.1. NOÇÃO

O conceito de Operação Bancária Aberta carece de previsão e definição legal. Contudo, o Decreto-Lei n.º 91/2018, de 12 de novembro, que aprova o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica ("RJSPME") e transpõe para a ordem jurídica interna a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 ("DSP 2"), relativa aos serviços de pagamento no mercado interno (segunda Diretiva de Serviços de Pagamento) determina, no seu Capítulo VIII, que regula sobre "Acesso a sistemas e contas de pagamento" e mais precisamente no artigo 69º, n.º 1, sob a epígrafe de "Acesso a contas detidas junto de uma instituição de crédito", que as "*instituições de crédito asseguram às instituições de pagamento e às instituições de moeda eletrónica, numa base objetiva, não discriminatória e proporcionada, o acesso aos serviços de pagamento referidos no artigo 4.º que sejam adequados a permitir que as instituições requerentes prestem serviços de pagamento de forma eficiente e sem entraves*". Ainda que a operação bancária aberta careça de uma definição legal, podemos retirar algumas conclusões da presente disposição.

Da referida norma podemos, em primeiro lugar, aferir que o legislador impôs às instituições de crédito[7] um dever de assegurar o acesso aos novos operadores no mercado. Daqui se retira a importância que o legislador europeu atribuiu a este tipo de serviços de pagamento. Um dos principais objetivos da União Europeia foi exatamente garantir a continuidade no mercado, permitindo que tanto os prestadores de serviços existentes como os novos prestadores de serviços de pagamento, independentemente do modelo de negócio, prestem os seus serviços no âmbito de um quadro regulamentar claro e harmonizado[8], bem como afirmar o desenvolvimento de novos tipos de serviços de

[7] Nos termos do Regime Jurídico das Instituições de Crédito e Sociedades Financeiras, aprovado pelo Decreto-Lei n.º 298/92, de 31 de Dezembro que transpõe para a ordem jurídica portuguesa as Diretivas n.º 77/780/CEE do Conselho, de 12 de Dezembro de 1989, na parte que, a coberto das derrogações acordadas, ainda não fora acolhida na legislação nacional, a Diretiva n.º 897/646/CEE do Conselho, de 15 de Dezembro de 1989 (Segunda Diretiva de Coordenação Bancária) e a Diretiva n.º 92/30/CEE do Conselho, de 6 de Abril de 1992, sobre supervisão das instituições de crédito em base consolidada e aprova o Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), na sua redação mais recente dada pela Lei n.º 58/2020 de 31 de agosto.

[8] *Vide* Considerando (33) da DSP 2.

pagamento, garantindo simultaneamente condições equivalentes para o exercício da atividade[9] e estimulando a intervenção de novos operadores e fomentando a concorrência entre *players* no mercado. Neste contexto, o legislador europeu não reconheceu este *acesso aos serviços de pagamento* como uma faculdade da instituição de crédito, mas sim, como um dever da instituição de crédito, perante o consentimento do cliente.

O acesso aos serviços de pagamento pressupõe o preenchimento de determinados critérios, sendo eles uma "*base objetiva, não discriminatória e proporcionada".* Esta norma que determina as condições de acesso por parte dos prestadores de serviços complementares às contas de pagamento dos utilizadores com recurso a conceitos indeterminados, fá-lo, no nosso entendimento, muito vagamente. Nas palavras do Professor MENEZES CORDEIRO *os conceitos dizem-se indeterminados por não permitirem comunicações claras quanto ao seu conteúdo*[10]. O mesmo autor caracteriza esta técnica legislativa como *polissemia, vaguidade, ambiguidade, porosidade e esvaziamento.* A utilização de um conjunto de conceitos indeterminados para descrever em que termos o acesso deve ser realizado, contribui para uma dificuldade acrescida no momento da apreciação e interpretação destes conceitos. A discricionariedade enquanto concessão por parte do legislador europeu de um poder próprio de fixação de critérios aos Estados membros, pode facilmente culminar numa fixação diferenciada dentro do seio da União Europeia, que naturalmente contradiz o objetivo de criação de um quadro legislativo geral europeu e de harmonizar a aplicação de regras sobre o serviço de pagamento e da conceção de um mercado único[11].

O n.º 2 do mesmo preceito determina que "*uma eventual recusa de acesso aos serviços de contas de pagamento carece de fundamentação, a qual deve ser comunicada pela instituição de crédito ao Banco de Portugal*". No mesmo sentido, refere o artigo 109º, n.º 1 do RJSPME que pode ocorrer uma recusa "*por motivos objetivamente justificados e devidamente comprovados relacionados com o acesso fraudulento ou não autorizado à conta de pagamento [...], incluindo a iniciação fraudulenta ou não autorizada de uma operação de pagamento"*. Contudo, a previsão, por parte do

[9] *Vide* Considerando (21) da DSP 2.
[10] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil I*, 4ª Ed. Almedina, 2012, p. 779
[11] Neste sentido, TIAGO DA CUNHA PEREIRA, *DSP 2: Oportunidades e Desafios,* in Revista de Direito Financeiro e dos Mercados de Capitais, Vol. 1, 2019, NO. 5, 507-524, p. 523, que questiona ainda se esta concretização não deveria ter impreterivelmente passado pela Autoridade Bancária Europeia.

legislador, de uma eventual recusa parece-nos ter sido propositada e acautelada. Quando o cliente bancário procura um serviço de pagamento novo e inovador, complementar aos serviços bancários prestados pela instituição de crédito, essa mesma vontade deve respeitar determinados critérios. O recurso a novos serviços de pagamento não pode deixar a instituição de crédito totalmente desprotegida face à intervenção de entidades terceiras na relação bancária previamente estabelecida. A *ratio legis* da previsão normativa de uma possível recusa de acesso aos serviços de contas de pagamento é a de dispor uma proteção adequada às instituições de crédito, noutras palavras, uma "válvula de escape", numa situação em que haja motivos objetivamente justificativos de tal recusa e quando esteja devidamente comprovado que os mesmos estejam relacionados com uma operação de natureza fraudulenta ou que careça da autorização do cliente/ utilizador do serviço. Desta forma a instituição de crédito goza de uma medida restritiva do acesso às contas de pagamento e à informação bancária, por parte de terceiros, na medida em que a DSP 2 parece, na maioria das vezes, favorecer o desenvolvimento de novos prestadores de serviços de pagamentos[12], como parece igualmente ter procurado um ponto de equilíbrio entre o incentivo à expansão e/ ou crescimento de novos intervenientes no mercado e um mecanismo de proteção às instituições de crédito já estabelecidas, garantindo simultaneamente condições equivalentes para o exercício da atividade tanto aos prestadores de serviços de pagamento existentes como aos novos prestadores. Ainda assim, o legislador vem exigir que na eventualidade de uma recusa a instituição tenha a diligência de comunicar ao prestador do serviço.

Pelo acima exposto, arriscamo-nos assim a definir a Operação Bancária Aberta como um modelo colaborativo[13], complementar aos habituais serviços de pagamento, que opera através da partilha de dados bancários, entre duas ou mais partes, através de interfaces de programação de aplicação[14][15], que correspondem a um método através do qual dois

---

[12] Cfr. Considerando (5) da DSP 2 determina *a presente diretiva deverá procurar garantir a continuidade no mercado, permitindo que tanto os prestadores de serviços existentes como os novos prestadores de serviços de pagamento, independentemente do modelo de negócio que apliquem, prestem os seus serviços no âmbito de um quadro regulamentar claro e harmonizado.*
[13] TIAGO CORREIA MOREIRA, *Partilha de dados pessoais e operação bancária aberta*, in FinTech - Desafios da Tecnologia Financeira, coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte Vol. 2, 1ª ed., Almedina, 2019, p. 148.
[14] Do inglês, *application programming interfaces.*
[15] LAURA BRODSKY e LIZ OAKES, *Data sharing and open banking,* artigo da Mckinsey & Company, 2017, *A partilha de dados é frequentemente realizada através de uma interface de programação de aplicação (API), uma conduta inteligente que permite o fluxo de dados entre sistemas de uma forma controlada, mas sem falhas. As APIs têm sido alavancadas em*

sistemas informáticos partilham dados[16]. O serviço opera através da colaboração entre o banco e a instituição de pagamento, na medida em que o primeiro partilha os dados bancários da conta de pagamento e do cliente ao segundo no âmbito de um modelo de colaboração[17]. O prestador do serviço complementar passa a deter a informação bancária necessária à prestação do seu serviço, reunindo assim as condições para a realização da ordem dada pelo utilizador do serviço. Esta operação pressupõe, naturalmente, o consentimento prévio do cliente na partilha dos dados bancários e na realização da operação de pagamento[18].

Falamos em serviços complementares, uma vez que, para estes se poderem realizar carecem da existência prévia de uma conta bancária junto de uma instituição de crédito e porque criam valor acrescentado na relação com os clientes pela forma inovadora como têm vindo a apresentar os seus serviços. É evidente que este tipo de serviços é somente possível com a evolução tecnológica, na medida em que se concretiza através do recurso a interfaces de programação de aplicação em linha do prestador de serviços de pagamento que gere as contas, i. é., uma API.

---

configurações bancárias durante anos. No entanto, dados os avanços na análise avançada e o impulso do mercado provocado por numerosas empresas fintech não bancárias, os APIs estão a receber atenção renovada como forma de melhorar a prestação de serviços financeiros tanto a consumidores retalhistas como a clientes empresariais, disponível em https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

[16] ANDREW BARBER, *Open banking will facilitate home loan switching*, artigo para a Pinsent Masons, 2017, refere que a *operação bancária aberta se traduz na prática de partilha de informação financeira por via eletrónica, com segurança, e apenas sob condição de consentimento dos utilizadores.* Disponível em: https://www.pinsentmasons.com/out-law/news/uk-moving-from-open-banking-to-open-finance

[17] Autoridade da Concorrência, *Inovação Tecnológica e Concorrência no Setor Financeiro em Portugal*, Issues Paper, 2018: *A iniciativa "Open Banking" consiste numa política de maior transparência nos serviços bancários, na avaliação da qualidade destes serviços e numa medida à época pioneira: a abertura das APIs dos bancos para que as empresas FinTech tenham acesso aos dados necessários ao desenvolvimento de novas soluções bancárias. A Competition and Markets Authority impos um remédio que implica a criação e financiamento, pelas principais instituições de crédito, de uma Entidade de Implementação (Implementation Entity) da iniciativa, encarregada de acordar, implementar e manter open banking standards comuns.*
A Competition and Markets Authority designou o "Implementation Trustee", encarregado de atuar como Chair e responsável pelos resultados dos objetivos estabelecidos para a Entidade de Implementação, na qual estariam representadas, através de grupos de stakeholders, as empresas FinTech, os bancos, os prestadores de serviços de pagamento e os consumidores. Disponível em: http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Estudos_Economicos/Banca_e_Seguros/Documents/Versão%20Final%20Issues%20Paper%20FinTech.pdf

[18] Adiante aprofundaremos esta tema.

A denominação "operação bancária aberta" encontra a sua justificação em duas vertentes; a primeira (i) pela entrada de novas entidades e de novos serviços de pagamento no mercado; e a segunda, (ii) pela criação de modelos que permitam que essas novas entidades consigam ter acesso aos sistemas e fazer uso da informação, entretanto armazenada pelos bancos[19]. Por um lado, assistimos a uma abertura do mercado em si, na medida em que os novos prestadores de serviços de pagamento entram no mercado e passam a ser reconhecidos pelo legislador europeu através da DSP 2. O mercado, que até então era predominantemente ocupado por incumbentes, vê-se agora obrigado a aceitar novos *players* servindo esta entrada de alavancagem e contribuindo para um sentido de concorrência e eficiência entre todos os agentes económicos. A entrada em vigor da DSP 2 franqueia as portas jurídicas e regulatórias do mercado dos serviços de pagamento a instituições especializadas em fases ou dimensões específicas dos serviços de pagamento[20], bem como a inovadores modelos de negócio através de meios tecnológicos.

Por outro lado, a operação bancária aberta obriga a uma abertura dos próprios sistemas dos bancos aos novos prestadores de serviços e à criação de modelos e infraestruturas técnicas. É essencial que os bancos concedam acesso por parte dos novos prestadores de serviços às contas de pagamento dos clientes e partilhem com estes a informação bancária necessária à prestação do serviço, entretanto armazenada pelas instituições de crédito. A "abertura" a que se refere a operação bancária assume um sentido figurativo, no sentido em que a instituição de crédito "se abre" perante os novos prestadores de serviços de pagamento, na medida em que disponibiliza os seus mecanismos de acesso direto ao prestadores de serviços de pagamento complementares e partilha informação bancária com os mesmos. Algo que até agora era somente detido pela instituição de crédito, passa a ser partilhado com uma entidade terceira à relação bancária com o cliente. Assim, a "abertura" da operação bancária materializa-se aquando do processo de recolha, arquivo, utilização e transmissão dos dados bancários e pressupõe que os bancos partilhem os dados que detêm sobre as contas de pagamentos dos seus clientes.

---

[19] TIAGO CORREIA MOREIRA, *Partilha de dados pessoais e operação bancária aberta*, in FinTech - Desafios da Tecnologia Financeira, coord. António Menezes Cordeiro, Ana Perestrelo de Oliveira, Diogo Pereira Duarte, Vol. 2, 1ª ed., Almedina, 2019, p. 148.

[20] FRANCISCO MENDES CORREIA, *Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*, in: III Congresso de direito bancário, Coimbra, 2017.

Por fim, esta "abertura" inclui igualmente um elemento tecnológico. A partilha de dados pode abranger uma necessidade de criação de modelos informáticos que permitam o acesso aos dados pelas novas entidades. Muitas vezes os dados que temos vindo a referir são algoritmos ou são anonimizados, ou até mesmo, encriptados. De maneira a que os novos *players* consigam ler e entender os dados é necessário haver uma estandardização destes dados, sob pena de a forma de o incumbente trabalhar e arquivar os dados ser diferente da forma como a nova entidade o faz e não conseguir, em última análise, realizar a leitura dos dados. É neste sentido que a União Europeia emanou variados Regulamentos Delegados[21] que complementam a Diretiva Europeia 2015/2366 e regulam este elemento tecnológico.

Uma discussão importante, neste âmbito, versa sobre o que são efetivamente dados bancários. Como se enquadram os dados bancários nos dados pessoais? Que dados bancários devem ser partilhados?

2.2. Dos Serviços de Pagamento

2.2.1. Introdução

A Diretiva Europeia 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007 ("DSP 1"), relativa aos serviços de pagamento no mercado interno é a primeira base legal europeia que regulamenta o tema dos serviços de pagamento. A grande novidade que a DSP 1 introduz no ordenamento jurídico europeu refere-se à consagração das instituições de pagamento[22]. Em Portugal a transposição da DSP 1 ocorreu através do Decreto-Lei n.º 317/2009, de 30 de outubro de 2009, o qual entrou em vigor no dia 1 de novembro de 2009. O Decreto-lei veio regular o acesso à atividade das

[21] Tais como o Regulamento Delegado (UE) 2017/2055 da Comissão, de 23 de junho de 2017, que completa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que diz respeito às normas técnicas de regulamentação para a cooperação e a troca de informações entre autoridades competentes relativamente ao exercício do direito de estabelecimento e da livre prestação de serviços das instituições de pagamento; e o Regulamento Delegado (UE) 2018/389 da Comissão de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

[22] FRANCISCO MENDES CORREIA, "*Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*", in III Congresso de direito bancário, Coimbra, 2017, p. 394.

instituições de pagamento e a prestação de serviços de pagamento a utilizadores desses mesmos serviços[23].

Durante a vigência da DSP 1 assistiu-se a um desenvolvimento do mercado único. O progressivo aumento da utilização de meios de pagamento eletrónicos ofereceu a possibilidade a novos prestadores de serviços de entrarem no mercado e apresentarem inovadores modelos de negócio. Paralelamente, observámos uma migração generalizada dos serviços de pagamento para ambientes eletrónicos[24]. A combinação destes dois fatores provocou uma insuficiente resposta a nível legislativo. A muito célere evolução tecnológica e os novos serviços de pagamento daí resultantes rapidamente viram a sua base legal desatualizada[25]. Atingiu-se uma situação em que novos modelos de negócio com inovadoras soluções tecnológicas deixaram de encontrar enquadramento e/ou reconhecimento na DSP 1[26]. A evidente lacuna legislativa pressionou o legislador europeu a proceder a uma revisão e criação de um quadro jurídico harmonizado que desse resposta às exigências da nova realidade dos serviços de pagamento. Em janeiro de 2012 a Comissão Europeia lançou um Livro Verde para um mercado europeu integrado dos pagamentos por cartão, por Internet e por telemóvel[27].

---

[23] *Vide* Uría Menéndez, A*lgumas Notas sobre a transposição da Diretiva de Serviços de Pagamento em Portuga*l, 2010, disponível em: https://www.uria.com/documentos/publicaciones/2517/documento/articuloUM.pdf?id=3030

[24] FRANCISCO MENDES CORREIA, "*Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*", in III Congresso de direito bancário, Coimbra, 2017, p. 388.

[25] Neste âmbito, o Considerando (28): *Desde a adoção da Diretiva 2007/64/CE, surgiram novos tipos de serviços de pagamento, nomeadamente no domínio dos pagamentos através da Internet. Em particular, registou-se uma evolução nos serviços de iniciação de pagamentos no domínio do comércio eletrónico. Esses serviços de pagamento têm um papel a desempenhar nos pagamentos efetuados no âmbito do comércio eletrónico criando uma ponte telemática entre o sítio web do comerciante e a plataforma bancária em linha do prestador de serviços de pagamento que gere as contas do ordenante, a fim de iniciar pagamentos através da Internet com base numa transferência a crédito.*

[26] Considerando (29) da DSP 2: *Atendendo a que os serviços de iniciação de pagamentos não estão atualmente abrangidos pela Diretiva 2007/64/CE, não são necessariamente supervisionados por uma autoridade competente nem estão obrigados a cumprir o disposto na Diretiva 2007/64/CE. Isto suscita toda uma série de questões jurídicas, nomeadamente em matéria de proteção dos consumidores, de segurança e de responsabilidade, bem como em matéria de concorrência e de proteção de dados, especialmente no que respeita à proteção dos dados do utilizador de serviços de pagamento em conformidade com as regras da União em matéria de proteção de dados. As novas regras deverão, por conseguinte, dar resposta a essas questões.*

[27] Bruxelas, 11.1.2012 COM(2011) 941 final. Disponível em: https://ec.europa.eu/transparency/regdoc/rep/1/2011/PT/1-2011-941-PT-F1-1.Pdf

O processo de revisão da DSP 1 deu origem a um pacote legislativo europeu sobre serviços de pagamento, composto por vários Diplomas[28], mas encabeçado pela Diretiva Europeia 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno. Para o ordenamento jurídico português a Diretiva Europeia 2015/2366 foi transposta através do Decreto-Lei n.º 91/2018, de 12 de novembro. A DSP 1 e a DSP 2 criam assim, conjuntamente, o modelo europeu dos serviços de pagamento.

A DSP 2 procurou assim reconhecer e criar um quadro jurídico claro e neutro dos serviços de pagamento, permitindo o desenvolvimento de novos tipos de serviços de pagamento, garantindo simultaneamente condições equivalentes para o exercício da atividade tanto aos prestadores de serviços de pagamento existentes como aos novos prestadores. A DSP 2 visou igualmente dar resposta ao aumento dos riscos de segurança, provocado pela maior complexidade e volume de pagamentos eletrónicos através de dispositivos móveis, mediante normas detalhadas que regulem os deveres dos intervenientes e zelem pelo elevado nível de proteção dos consumidores.

O conceito de "serviço de pagamento" vem definido no n.º 3 do artigo 4.º da DSP 2, que, remetendo para o Anexo I da Diretiva, determina tratar-se de uma atividade comercial constante no mesmo anexo, ou várias dessas atividades[29]. O conceito de "serviço de pagamento" foi inicialmente definido no n.º 3 do artigo 4.º da DSP 1. Uma comparação entre ambos os Diplomas, permite concluir que o conceito em geral não sofreu grandes alterações. Contudo, a DSP 2 ao invés da DSP 1 prevê dois novos tipos de serviços de pagamento: o serviço de iniciação do pagamento e o serviço de informação sobre contas[30].

[28] Conforme referidos anteriormente.
[29] Sobre a definição de serviços de pagamento, pode ler-se no Considerando (21) da DSP 2 que a *"definição de serviços de pagamento deverá ser tecnologicamente neutra e deverá permitir o desenvolvimento de novos tipos de serviços de pagamento, garantindo simultaneamente condições equivalentes para o exercício da atividade tanto aos prestadores de serviços de pagamento existentes como aos novos prestadores"*.
[30] Aprofundaremos este tema adiante.

2.2.2. DAS ALTERAÇÕES INTRODUZIDAS PELA DIRETIVA EUROPEIA 2015/2366

Antes da entrada em vigor da DSP 2, muitos produtos ou serviços de pagamento inovadores não estavam abrangidos, na sua totalidade ou em grande parte, pelo âmbito de aplicação da DSP 1. Além disso, o âmbito de aplicação da DSP 1 e, em especial, os elementos dele excluídos, tais como determinadas atividades conexas aos pagamentos, revelavam-se, nalguns casos, demasiado ambíguos, demasiado gerais ou simplesmente desatualizados, atendendo à evolução do mercado. Esta situação gerou insegurança jurídica, riscos potenciais para a segurança da cadeia de pagamentos e falta de proteção dos consumidores em determinados domínios. Os prestadores de serviços de pagamento eram confrontados com dificuldades para lançarem serviços de pagamento por meios digitais, inovadores, seguros e de fácil utilização e para oferecerem aos consumidores e retalhistas métodos de pagamento eficazes, práticos e seguros na União Europeia.

Afigurava-se essencial uma revisão do quadro legislativo, de maneira a colmatar as lacunas regulamentares, assegurando simultaneamente uma maior clareza jurídica e uma aplicação coerente em todos os Estados membros. Garantir aos operadores já presentes no mercado e aos novos operadores condições equivalentes para o exercício da atividade, permitindo a implantação generalizada dos novos meios de pagamento no mercado e garantindo um elevado nível de proteção dos consumidores na utilização desses serviços de pagamento em toda a União era absolutamente fulcral.

Até à entrada em vigor da DSP 2 era evidente o tratamento desigual entre os prestadores de serviços complementares e os incumbentes, bem como os direitos e obrigações diferenciados a que estes estavam sujeitos. Nas palavras de FRANCISCO MENDES CORREIA *a ausência de um enquadramento jurídico claro para novos prestadores e novos serviços era criticada pelos tradicionais prestadores de serviços de pagamento, perante a possibilidade de concorrência de novos atores que não enfrentavam custos regulatórios e de compliance comparáveis, mas também pelos novos agentes, que muitas vezes viam negado o acesso às infraestruturas de pagamentos (necessárias para a participação no mercado), com fundamento precisamente na falta de regulação específica da sua atividade*[31]. A revisão do quadro jurídico permitiu determinar regras e prever medidas mais eficientes e adequadas em matéria de transparência e

[31] FRANCISCO MENDES CORREIA, "*Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*", in III Congresso de direito bancário, Coimbra, 2017, p. 388

requisitos de informação aplicáveis aos prestadores de serviços de pagamento e em matéria de direitos e obrigações relacionados com a prestação e utilização de serviços de pagamento. A entrada em vigor da DSP 2 permitiu desta forma corrigir estas situações menos claras.

Uma das principais novidades foi o reconhecimento de novos intervenientes no mercado – os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de informação sobre contas. A revisão do quadro jurídico permitiu essencialmente gerar eficiências em todo o sistema de pagamentos e traduzir-se numa maior escolha e numa maior transparência no domínio dos serviços de pagamento, reforçando simultaneamente a confiança dos consumidores num mercado de pagamentos harmonizado.

Importa acrescentar que a entrada de novos operadores no mercado provocou, de forma evidente, um espírito de concorrência entre os agentes económicos. O mercado que até agora era predominantemente ocupado por operadores já posicionados no mercado, assistiu a um aumento do número de *players* e a implantação dos novos meios de pagamento no mercado. Com a oferta de serviços mais simples, céleres e gratuitos e de um processo de operações de pagamento otimizado, os clientes tornaram-se mais exigentes na oferta e na qualidade dos serviços prestados. Os operadores já presentes no mercado viram-se assim obrigados a inovar tecnologicamente, bem como a nível dos modelos de negócio que apresentavam aos seus clientes. Os incumbentes passaram a ter de incorporar nos seus serviços financeiros soluções tecnológicas. A partilha da quota de mercado com os novos intervenientes obrigou nos últimos anos, os incumbentes a modernizarem os serviços que apresentam aos seus clientes, sob pena de serem ultrapassados pela nova realidade mais tecnológica e simples. Em última análise a abertura do mercado a intervenientes inovadores promoveu uma eficiência e uma melhoria na oferta de serviços de pagamento e na relação entre os agentes económicos e entre os prestadores de serviços e os seus clientes.

Neste âmbito, surgiu uma grande dúvida no sentido de aferir se a intervenção de novas entidades seria num plano disruptivo para os incumbentes ou, se por ventura, seria num plano colaborativo[32].

[32] Adiante profundaremos este tema.

Como já referimos uma novidade introduzida pela DSP 2 foi o reconhecimento de serviços de pagamento complementares. Desde a adoção da DSP 1, e graças à evolução tecnológica, surgiram ao longo dos últimos anos novos tipos de serviços de pagamentos – serviços de iniciação de pagamento e os serviços de informação sobre contas – sendo estes prestados de forma complementar aos habituais serviços de pagamento.

Um primeiro serviço é o serviço de iniciação de pagamento, que permite ao prestador do serviço assegurar ao beneficiário do pagamento/comerciante, que o pagamento seja iniciado, a fim de incentivar o beneficiário do pagamento/comerciante a disponibilizar o bem ou a prestar o serviço sem demora indevida[33].

Num primeiro momento, e a primeira ação que desencadeia o processo em questão, é a ordem de pagamento dada pelo utilizador do serviço diretamente ao prestador do serviço de iniciação de pagamento, referente a uma conta de pagamento detida por uma instituição de crédito. O prestador do serviço de iniciação do pagamento, perante a ordem do utilizador, verifica, mediante autorização, os dados da conta de pagamento e se existem fundos disponíveis para efetuar o pagamento. Em caso afirmativo o prestador do serviço de iniciação do pagamento, partilha a informação de saldos suficientes com instituição de crédito que, de seguida, inicia a ordem de pagamento. Por sua vez, a instituição de crédito informa o prestador do serviço de iniciação do pagamento que a operação de pagamento foi realizada. O prestador do serviço de iniciação assegura, posteriormente, o beneficiário que o pagamento foi iniciado, a fim de incentivar o beneficiário a disponibilizar o bem ou a prestar o serviço sem demora indevida. Perante esta informação o comerciante disponibiliza o bem ou serviço ao consumidor.

A DSP 2 descreve esta intervenção do prestador do serviço de pagamento como uma "*ponte telemática entre o sítio web do comerciante e a plataforma bancária em linha do prestador de serviços de pagamento que gere as contas do ordenante*"[34].

A adoção da DSP 2 introduziu outro novo serviço de pagamento: os serviços de informação sobre contas. Neste serviço o utilizador acede a uma interface, criada por uma entidade prestadora do serviço de pagamento de informação sobre contas que, por sua vez, consulta a informação sobre uma ou mais contas de pagamento detidas pelo

[33] *Vide* Considerando (29) da DSP 2
[34] *Vide* Considerando (27) da DSP 2.

utilizador, junto de um ou mais prestadores de serviços de pagamento (entidade bancária)[35]. Depois de consultada a informação sobre as contas de pagamento, o prestador de serviços coloca para consulta do utilizador a informação a que acedeu, por via da interface. Noutras palavras, o utilizador ao consultar esta interface tem à sua disposição uma agregação dos saldos das suas contas de pagamento e uma *visão global da sua situação financeira num dado momento*[36].

Estão em causa dois serviços de pagamento complementares aos serviços de prestação de pagamento *core* realizados pelos incumbentes. São serviços que necessitam, por base, da já existência de uma conta de pagamento e, naturalmente, de um prestador de serviços de pagamento que disponibilize e gira a conta de pagamento do utilizador. Estamos a falar de entidades que, em regra, não detêm fundos dos clientes e não têm competência para os movimentar, gerir ou disponibilizar. Têm, sim, acesso à informação que consta nas contas de pagamento, uma vez que prestam serviços tecnológicos, que pressupondo o conhecimento da situação financeira do utilizador.

A relação estabelecida entre os novos intervenientes e os incumbentes, no âmbito dos novos serviços de pagamento reconhecidos pela DSP 2, foi, igualmente, alvo de regulação. Na referida relação, de maneira a assegurar a segurança e a transparência, os intervenientes estão sujeitos a normas comuns e abertas de comunicação. Estas normas pretendem, no fundo, garantir a interoperabilidade de diferentes soluções tecnológicas de comunicação, assim como garantir que o prestador do serviço de pagamento que gere a conta se encontra ciente de que o contacto com ele estabelecido é efetuado por um prestador de serviços de iniciação de pagamentos ou por um prestador de serviços de informação sobre contas e não pelo próprio cliente. Estas normas devem, igualmente, garantir que os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de informação sobre contas comuniquem de forma segura com o prestador do serviço de pagamento que gere a conta e com os clientes em causa[37].

Acrescido a estas normas, o Parlamento Europeu e o Conselho encarregam a Autoridade Bancária Europeia ("EBA") de elaborar normas técnicas de regulamentação. Neste sentido, foi emanado o Regulamento Delegado (UE) 2018/389 da Comissão de 27

[35] *Vide* artigo 4.º, n.º 17.
[36] *Vide* Considerando (28) da DSP 2.
[37] *Vide* Considerando (93) da DSP 2.

de novembro, sobre autenticação forte do cliente e normas abertas de comunicação comuns e seguras, complementando o pacote legislativo sobre a matéria dos serviços de pagamento.

As normas abertas de comunicação comuns e seguras vêm, neste sentido, procurar impor uma obrigação de observar os requisitos sobre a proteção dos utilizadores dos serviços em causa e da segurança das operações efetuadas, um tratamento equitativo entre os prestadores de serviços, submetendo todos os intervenientes a normas semelhantes, a critérios de transparência e ainda de forma a assegurar um elemento tecnológico comum a todos.

2.3. Da Estrutura Contratual no âmbito da Operação Bancária Aberta

A realização de uma operação, no âmbito da operação bancária aberta, pressupõe uma intervenção tripartida – o cliente/utilizador; o banco; e a instituição de pagamento. Na verdade, dos três intervenientes na operação bancária, apenas se estabelecem duas relações contratuais, nomeadamente, entre o banco e o seu cliente, por um lado, e o utilizador do serviço e o prestador do serviço de pagamento, por outro. Entre a instituição de pagamento e a instituição de crédito não existe obrigatoriamente uma relação contratual. A prestação do serviço de pagamento não está dependente de uma relação contratual prévia entre os prestadores de serviços de pagamento e os prestadores de serviços de pagamento que gerem contas.

A celebração dos dois contratos mencionados, permite de antemão estabelecer a relação contratual entre os intervenientes e definir os direitos e obrigações que vigorarão durante a vigência da relação contratual, desta maneira simplificando o procedimento no momento de futuras operações de pagamento.

2.3.1. Da Relação Contratual entre o Cliente e a Instituição de Crédito

Os serviços de pagamento, no âmbito da operação bancária aberta, são serviços complementares aos serviços de pagamento *core* prestados pelas instituições de crédito. Trata-se de serviços complementares, na medida em que auxiliam ou complementam essa prestação de serviços tipicamente prestados pelas instituições de crédito. Referimo-nos, nesta medida, à receção de depósitos ou outros fundos reembolsáveis, operações de

crédito, incluindo a concessão de garantias e outros compromissos, locação financeira e *factoring*, serviços de pagamento, emissão e gestão de meios de pagamento, entre outros.

Posto isto, justifica-se esta natureza complementar dos novos serviços de pagamento introduzidos pela DSP 2, uma vez que, para operarem, os prestadores dos serviços de pagamento complementares carecem da existência de fundos que, por sua, vez, são detidos e geridos por instituições de crédito.

Assim, pressupõe-se a existência de uma relação contratual bancária prévia entre a instituição de crédito e a cliente. A relação inicia-se com a celebração de um contrato de abertura de conta. O contrato de abertura de conta é um negócio jurídico que marca o início de uma relação bancária complexa entre o banqueiro e o cliente e traça o quadro básico do relacionamento entre tais entidades[3839].

O contrato de abertura de conta[40] pretende, no âmbito de uma relação duradoura, estabelecer as obrigações das partes[41] e as condições de realização dos atos posteriores, com base no qual se estabelecerão inúmeros contratos bancários no futuro. Neste sentido, poder-se-á definir o contrato de abertura de conta como um contrato-quadro[42], na medida em que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento[43].

Desta forma, fortemente interligado à abertura de conta está o contrato de depósito bancário. O contrato de depósito bancário é um contrato "mediante o qual o *tradens* aceita

---

[38] Ac. Supremo Tribunal de Justiça ("STJ"), de 07-10-2010, com o relator Serra Baptista, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/7e6e904d4d57102c802577b500560396?OpenDocument

[39] Neste sentido, ANTÓNIO MENEZES CORDEIRO, Manual de Direito Bancário, 4ª edição, Almedina, 2010, pp. 260-264, 505-511

[40] Atente-se ao Aviso do Banco de Portugal n.º 11/2005, alterado pelo Aviso n.º 2/2007, que determina que o contrato de abertura de conta "*constitui uma operação bancária central pela qual se inicia, com frequência, uma relação de negócio duradoura entre o cliente e a instituição de crédito, a qual requer um conhecimento, tanto quanto possível, completo, seguro e permanentemente atualizado dos elementos identificadores do cliente, dos seus eventuais representantes e de quem movimenta a conta*"

[41] MARIA JOÃO RODRIGUES, "Depósito bancário", in: Temas de Direito Bancário, N.º 9, 2014, p. 270.

[42] Nos termos do artigo 2º do RJSPME define-se como *um contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento.*

[43] *Vide* alínea i) do Artigo 2.º da DSP 2.

transferir a propriedade de um bem (fungível) para a esfera de domínio de outrem (*accipiens*) que dela pode dispor com a obrigação de a restituir sempre e quando lhe for exigida[44].

Celebrados estes contratos entre o cliente e a instituição de crédito, o cliente é titular de uma conta bancária aberta e fundos disponíveis, tendo a liberdade para realizar quaisquer operações de pagamento previstas no contrato ou na legislação aplicável.

2.3.1.1. DO SIGILO BANCÁRIO

O sigilo bancário é um dever subjacente à relação contratual que se estabelece entre o cliente e a instituição de crédito, acompanhando desde sempre a profissão do banqueiro[45]. Ao longo dos tempos o sigilo bancário tem ganho cada vez maior relevância, tendo na altura do seu surgimento assumido um papel de mero costume[46], passando depois a constituir um verdadeiro dever de não revelar determinados conhecimentos ou informações[47] previsto por lei. Em Portugal o conceito de sigilo bancário foi primeiramente estabelecido pelo Regulamento Administrativo do Banco de Portugal, aprovado pelo Decreto de 25 de janeiro de 1847[48], seguindo-se depois disso uma série de previsões legais deste dever em diferentes diplomas. Mais recentemente em Portugal, apenas depois do 25 de abril de 1974, com a instabilidade que o país atravessava o

---

[44] Ac. STJ, de 10-11-2011, com o relator Gabriel Catarino, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/4e38c7ac3718495b8025794a004f2897?OpenDocument

[45] ANTÓNIO MENEZES CORDEIRO, *Direito Bancário*, 5ª ed. rev. e atualizada, Almedina, 2014, pp. 345.

[46] ANA SOFIA LOPES VAZ, *O acesso a informações bancárias e financeiras por parte da Autoridade Tributária e Aduaneira. O fim do sigilo bancário?*, Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto, 2017 p. 2, escreve que *durante o período do Império Romano, o segredo bancário encontra-se implicitamente abrangido através da actio iniuriarum, tendência que continua a ser mantida na Idade Média pelos Templários e banqueiros judeus enquanto costume jurídico e alma do comércio. No entanto, é durante a época do Renascimento que o segredo bancário começa a ganhar expressão entre os banqueiros protestantes, particularmente após a célebre carta sobre a usura de Calvino, em meados do séc. XVI. Porém, a conceção moderna do segredo bancário apenas viria a ter a sua consagração já em pleno séc. XX.*

[47] ANTÓNIO MENEZES CORDEIRO, Manual de direito bancário, 4º Edição, Almedina, Coimbra, 2010, p. 327

[48] Ac. do Tribunal da Relação de Coimbra de 28.11.2018 Processo n.º 1771/18.3T8PBL-B.C1 Relator Carlos Moreira, disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/df666253f908aa288025837c0053cdf8

legislador sentiu a necessidade de reforçar a tutela legal atribuída, tendo assim o sigilo bancário vindo a ser alvo consagrado em diferentes diplomas[49].

Hoje em dia, o sigilo bancário vem consagrado no Regime Geral das Instituições de Crédito e Sociedades Financeiras[50] ("RGICSF") e abrange *informações sobre factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços* estando sujeitos a este dever os *membros dos órgãos de administração ou fiscalização das instituições de crédito, os seus colaboradores, mandatários, comissários e outras pessoas que lhes prestem serviços a título permanente ou ocasional*[51]. Continua o n.º 2 do mesmo artigo que *estão sujeitos a segredo os nomes dos clientes, as contas de depósito e seus movimentos e outras operações bancárias.* Porém, são admitidas algumas exceções ao dever de segredo nomeadamente *os factos ou elementos das relações do cliente com a instituição podem ser revelados mediante autorização do cliente, transmitida à instituição*[52]*, entre outras*[53].

---

[49] SÉRGIO MANUEL BASTO CÂNDIDO SERDOURA DE MIRANDA, *O Segredo Bancário e a Administração Tributária,* Trabalho Final no III Curso de Pós-Graduação em Direito Fiscal, 2007, p. 5 refere que *o segredo bancário foi legalmente consagrado, em 1975, através da Lei Orgânica do Banco de Portugal, aprovada pelo Decreto-Lei n.º 644/75, de 15 de Novembro, e reforçado pelo Decreto-Lei n.º 729-F/75, de 22 de Dezembro, que consagrou as Bases Gerais das Instituições Bancárias Nacionalizadas. O segredo bancário foi, ainda, visado com o Decreto-Lei n.º 475/76, de 16 Julho, com a redação que deu ao n.º 1 do art. 290.º, do Código Penal, passando a penalizar a violação do segredo, surgindo, aqui, o segredo bancário na dependência do segredo profissional. Com o Decreto-Lei n.º 2/78, de 9 de Janeiro, proibiu-se a revelação de informação bancária. Poucos anos mais tarde, a legislação passa a estabelecer exceções, como, por exemplo, a Lei n.º 45/86, de 1 de Outubro, que dava poderes à Alta Autoridade contra a Corrupção para obter informações, mas restringia essa capacidade ao que não estivesse abrangido por dever de sigilo protegido pela lei.*

[50] Decreto-Lei n.º 298/92, de 31 de dezembro que aprova o Regime Geral das Instituições de Crédito e Sociedades Financeiras.

[51] N.º 1 do artigo 78º do RGICSF.

[52] N.º 1 do artigo 79º do RGICSF.

[53] Continua o n.º 2 do artigo 79º do RGICSF que *fora do caso previsto no número anterior, os factos e elementos cobertos pelo dever de segredo só podem ser revelados:*
a) Ao Banco de Portugal, no âmbito das suas atribuições;
b) À Comissão do Mercado de Valores Mobiliários, no âmbito das suas atribuições;
c) À Autoridade de Supervisão de Seguros e Fundos de Pensões, no âmbito das suas atribuições;
d) Ao Fundo de Garantia de Depósitos, ao Sistema de Indemnização aos Investidores e ao Fundo de Resolução, no âmbito das respetivas atribuições;
e) Às autoridades judiciárias, no âmbito de um processo penal;
f) Às comissões parlamentares de inquérito da Assembleia da República, no estritamente necessário ao cumprimento do respetivo objeto, o qual inclua especificamente a investigação ou exame das ações das autoridades responsáveis pela supervisão das instituições de crédito ou pela legislação relativa a essa supervisão;

Se atendermos ao disposto no artigo 78º do RGICSF percebemos que a operação bancária aberta e a partilha de informação na prestação dos novos serviços de pagamento entre entidades abrange exatamente a informação que o dever de segredo pretende tutelar, nomeadamente informações sobre factos ou elementos respeitantes às relações das instituições de crédito com os seus clientes e informações que decorram da prestação dos serviços comuns. Parece-nos estarmos estaremos perante dois diplomas contraditórios, no sentido em que um consagra um dever de segredo dos dados bancários adquiridos na relação contratual, e outro determina que instituições de crédito asseguram aos prestadores de serviços complementares, numa base objetiva, não discriminatória e proporcionada, o acesso aos serviços de pagamento de iniciação do pagamento e de informação sobre contas. Havendo esta contradição faz sentido questionar se não estará o dever de segredo ultrapassado tendo em conta esta nova realidade. Preocupação diversa é a falta de previsão dos prestadores dos serviços de pagamento complementares nas exceções elencadas no n.º 2 do artigo 79º do RGICSF. Cremos na necessidade de revisão do RGICSF neste aspeto, na medida em que não está de forma correta a dar resposta à nova realidade no mercado dos serviços de pagamento.

Importa ainda salientar que embora a informação prestada no âmbito da operação aberta não seja objeto das exceções ao dever de segredo previstas, o RGICSF estabelece no artigo 79º, sob a epígrafe de *Exceções ao dever de segredo*, que *os factos ou elementos das relações do cliente com a instituição podem ser revelados mediante autorização do cliente, transmitida à instituição*[54]. Ainda assim, o procedimento de autenticação forte do cliente traduz-se num procedimento que inclui, de um modo geral, mecanismos de controlo das operações para detetar tentativas de utilização das credenciais de segurança personalizadas de um utilizador de um serviço de pagamento que tenham sido perdidas, furtadas ou objeto de apropriação abusiva e deve igualmente assegurar que o utilizador do serviço de pagamento é o utilizador legítimo, sendo que nessa qualidade, consente a transferência de fundos e o acesso à informação sobre a sua conta através de uma utilização normal das credenciais de segurança personalizadas[55]. Posto isto parece-nos

g) À administração tributária, no âmbito das suas atribuições;
h) Quando exista outra disposição legal que expressamente limite o dever de segredo.

[54] Teremos oportunidade de aprofundar o tema da autenticação forte do cliente adiante.

[55] Regulamento Delegado (UE) 2018/389 de 27 de novembro de 2017 sobre normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

que todos os requisitos previstos do n.º do artigo 79.º estão cumpridos para serviços de iniciação do pagamento ou de informação sobre contas na exceção ao dever de segredo.

Para concluir, chamamos a atenção para o referido no Acórdão do Tribunal da Relação de Lisboa[56] que determina que *os valores protegidos pelo sigilo bancário são, por um lado, o regular funcionamento da atividade bancária, baseada num clima generalizado de confiança e segurança nas relações entre os bancos e seus clientes e o direito à reserva da vida privada desses clientes.* Continua o mesmo Tribunal que c*onquanto encontrando arrimo constitucional o direito ao sigilo bancário não é um direito absoluto*. Seguimos a opinião do referido Acórdão na medida em que o dever de segredo tem como corolário a proteção da atividade bancária desenvolvida pelas instituições de crédito e dos dados bancários. O dever de segredo mantém-se um pilar importante do desenvolvimento da atividade bancária e da segurança da informação bancária[57], que deve ser mantido e respeitado. Não cremos tratar-se de um dever desatualizado, mas sim, de um dever que deve moldar-se e adaptar-se em função da evolução e mudança do mercado financeiro, neste caso, provocada pela digitalização dos serviços financeiros.

2.3.2. Da Relação Contratual entre o Utilizador e o novo Prestador de Serviços de Pagamento

Num momento posterior à celebração dos referidos contratos entre o cliente e a instituição de crédito, o cliente pode recorrer a serviços de pagamento complementares prestados por instituições de pagamento. As instituições de pagamento[5859] são entidades de escopo limitado[60], tendo por objeto a prestação de um ou de mais serviços de pagamento[61] pouco onerosos, cómodos e que proporcionem uma experiência

[56] Ac. da Relação de Lisboa de 9 de fevereiro de 2017, Processo n.º 19498/16.9T8LSB-A.L1-2, Relator Ezaguy Martins, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/f774e277ee052c28802580d700589d0b?OpenDocument

[57] No artigo da Mckinsey & Company, LAURA BRODSKY e LIZ OAKES, *Data sharing and open banking*, 2017, defendem que um dos maiores ativos das instituições de crédito neste momento são os dados bancários sobre os seus clientes.

[58] Previstas pela primeira vez na DSP 1 e no Decreto Lei n.º 317/2009 de 30 de outubro.

[59] No n.º 4 do artigo 4º do Decreto Lei n.º 317/2009: *as pessoas colectivas a quem tenha sido concedida autorização para prestar e executar serviços de pagamento em toda a Comunidade.*

[60] FRANCISCO MENDES CORREIA, "*Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*", in III Congresso de direito bancário, Coimbra, 2017, p. 394.

[61] Para atividades acessórias que podem ser exercidas pelas instituições de pagãmente, *vide* n.º 2 do artigo 8º do Decreto Lei n.º 317/2009.

descomplicada e integrada ao utilizador. Contudo, estas entidades apenas podem prestar serviços de pagamento de forma limitada, não podendo deter fundos dos utilizadores, mas apenas obter informação sobre as mesmas ou um acesso muito limitado.

Para que o fornecimento desses serviços de pagamento seja possível, é necessária a celebração de um contrato prévio de prestação de serviço de pagamento de carácter isolado entre o utilizador do serviço e o prestador do mesmo.

Uma das principais características do contrato de prestação de serviço de pagamento de carácter isolado é o fator da distância, uma vez que a sua formação e conclusão são efetuadas exclusivamente através de canais digitais – a interface de programação – criada e organizada pelo prestador de serviços de pagamento para esse efeito. Outro aspeto particular deste contrato é ser prestado de forma episódica e a relação obrigacional estabelecida para esse propósito se limitar à execução da operação e a alguns deveres[62] *post finitum* que possam emergir[63].

O contrato de prestação de serviços vem, por sua vez, estipulado no artigo 1154.º do CC e define-se como aquele contrato em que uma das partes se obriga a proporcionar à outra, certo resultado do seu trabalho intelectual ou manual, com ou sem retribuição.

Já no âmbito da DSP 2, as operações realizadas no âmbito de um serviço de pagamento complementar inserem-se nas operações de pagamento de carácter isolado. O título iii do RJSPME trata da prestação e utilização de serviços de pagamento e subdivide-se em 3 Secções, sendo elas sobre (i) Regras Gerais; (ii) Operações de pagamento de carácter isolado; e (iii) Contratos-quadro. O artigo 85º (Informações a prestar ao ordenante e ao beneficiário após a iniciação de uma ordem de pagamento) insere-se na Secção (ii) sob a epígrafe de Operações de pagamento de carácter isolado do Capítulo II do Título III do RJSPME.

Esta inserção sistemática pelo legislador não é despropositada na medida em que o artigo 85.º não se insere no âmbito da Secção I, que se aplica a todos os tipos de operações de pagamento, sejam elas de caráter isolado, os próprios contratos-quadro e as por estes

[62] Estudaremos adiante no ponto 2.4.3.
[63] FRANCISCO MENDES CORREIA, *Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica*, in: Revista de Direito Civil, p. 704.

abrangidas, mas sim na Secção II exclusivamente sobre Operações de pagamento de carácter isolado. A Secção II aplica-se a operações de pagamento de carácter isolado não abrangidas por um contrato-quadro, conforme refere no n.º 1 do artigo 82.º.

2.4. DAS OBRIGAÇÕES DAS PARTES

A segurança dos pagamentos eletrónicos afigura-se como um aspeto fundamental para assegurar a proteção dos utilizadores e a promoção adequada do desenvolvimento do comércio eletrónico em condições concorrenciais. Na sequência do trabalho feito pela DSP 1, a DSP 2 veio aprofundar e aumentar a quantidade de deveres subjacentes aos prestadores dos serviços de pagamento, garantindo um elevado nível de proteção dos consumidores na utilização dos serviços.

O RJSPME regula no seu Título iii os deveres de informação pré-contratual e contratual, que impendem sobre as partes desta relação tripartidas, destinados a garantir a transparência das condições e dos requisitos de informação e normas que devem conformar os direitos e as obrigações na prestação e utilização de serviços de pagamento.

Propomo-nos neste capítulo a estudar os deveres subjacentes à operacionalização de pagamentos de forma a garantir a segurança das operações de pagamento e a proteção dos clientes contra riscos de fraude, bem como as regras de acesso à conta de pagamentos dos utilizadores e os respetivos limites, para que este se processe em segurança.

2.4.1. DEVERES DA INSTITUIÇÃO DE CRÉDITO

1. Assegurar o acesso à conta de pagamento em caso de serviços de iniciação do pagamento;

Se atentarmos a letra do artigo 69º, n.º 1 da DSP 2, observamos a principal obrigação que recai sobre o prestador de serviços de pagamento que gere a conta. Determina o artigo que as *instituições de crédito asseguram às instituições de pagamento e às instituições de moeda eletrónica, numa base objetiva, não discriminatória e proporcionada, o acesso aos serviços de pagamento referidos no artigo 4.º que sejam adequados a permitir que as instituições requerentes prestem serviços de pagamento de forma eficiente e sem entraves*. Ao abrigo deste artigo o prestador de serviços que gere a conta tem o dever de

assegurar o acesso dos serviços de pagamento previstos no artigo 4º do mesmo Diploma às instituições de pagamento, sendo que para efeitos do nosso estudo importam os serviços de iniciação de pagamento[64] e de informação sobre contas[65].[66]

A partilha dos dados bancários solicitados à instituição de pagamento, constitui um pressuposto essencial à prestação dos serviços de pagamento requeridos pelo cliente. Trata-se de uma conduta imprescindível, no âmbito da operação bancária aberta, na medida em que o prestador do serviço de pagamento apenas consegue fornecer os serviços, através da verificação dos saldos das contas de pagamento do cliente.

Atendendo aos dois tipos de serviços de pagamento introduzidos pela DSP 2, importa verificarmos em que termos é efetuada a partilha dos dados bancários. No âmbito da prestação de serviços de iniciação de pagamento, conforme referido anteriormente, é em primeiro lugar dada uma ordem de pagamento, que, *per si*, desencadeia o processo. Confrontado com esta ordem de pagamento, o prestador do serviço de iniciação de pagamento comunica à instituição de crédito e informa sobre a referida ordem de pagamento. Imediatamente após a receção da ordem de pagamento, a instituição de crédito, disponibiliza ao prestador do serviço de iniciação de pagamento as informações necessárias à iniciação da operação.

Desta forma, o prestador do serviço de iniciação do pagamento verifica se o utilizador detém os fundos necessários e disponíveis na conta de pagamento, da qual deve ser disponibilizado o valor necessário para realizar a operação de pagamento. Ora, é mediante a disponibilização da informação, por parte da instituição de crédito ao prestador do

[64] Vide artigo 4.º, g) do RJSPME.
[65] Vide artigo 4.º, h) do RJSPME.
[66] Considerando (20) do Regulamento Delegado 2018/389: *Cada prestador de serviços de pagamento gestor de contas que tenha contas de pagamento acessíveis em linha deve oferecer pelo menos uma interface de acesso que permita uma comunicação segura com os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões. A interface deve permitir que os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões se identifiquem junto do prestador de serviços de pagamento gestor de contas. De igual modo, a interface deve permitir que os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos se baseiem nos procedimentos de autenticação facultados pelo prestador de serviços de pagamento gestor de contas ao utilizador de serviços de pagamento.*

serviço de iniciação de pagamento que este último verifica se o utilizador detém fundos suficientes para dar início àquela ordem de pagamento.

Igualmente, no caso dos serviços de informação sobre contas, o utilizador acede a uma plataforma, de maneira a consultar a informação de uma ou mais contas bancárias de forma agregada. Também aqui o prestador do serviço de pagamento que gere a conta tem o dever de assegurar o acesso ao prestador do serviço de informação sobre contas. Apenas mediante o acesso à informação sobre os saldos bancários do utilizador, pode o prestador do serviço prestar esse serviço. Sem a informação em causa o prestador do serviço de informação estaria impossibilitado de prestar o serviço.

Apesar de existir este dever, importa salientar que o prestador de serviços de pagamento que gere a conta não apresenta obrigatoriamente uma relação contratual com prestadores de serviços de informação sobre contas ou os prestadores de serviços de iniciação de pagamento. A prestação dos serviços não depende de uma relação contratual entre a instituição de crédito e a instituição de pagamento.

2. Comunicar de forma segura com os prestadores de serviços de pagamento;

Conforme já referimos, existe uma comunicação indispensável entre o prestador de serviços de pagamento que gere a conta e os prestadores de serviços de informação sobre contas[67] e de iniciação de pagamento[68]. De forma a garantir a segurança da comunicação, o prestador de serviços de pagamento que gere a conta tem o dever de facultar um canal de comunicação seguro, entre os intervenientes relevantes[69], no contexto dos serviços de

[67] *Vide* artigo 107º, n.º 3, a) e n.º 5 do RJSPME.
[68] *Vide* artigo 106º, n.º 4 a) e n.º 6 do RJSPME.
[69] Vide para o efeito o Considerando (20) do Regulamento Delegado (UE) 2018/389 que determina que "*Cada prestador de serviços de pagamento gestor de contas que tenha contas de pagamento acessíveis em linha deve oferecer pelo menos uma interface de acesso que permita uma comunicação segura com os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões. A interface deve permitir que os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões se identifiquem junto do prestador de serviços de pagamento gestor de contas. (...) A fim de assegurar a neutralidade tecnológica e do modelo de negócio, os prestadores de serviços de pagamento que gerem as contas devem ser livres de decidir se oferecem uma interface dedicada à comunicação com os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões, ou se permitem, para essa comunicação, a utilização da interface para efeitos de identificação e comunicação com os*

informação sobre contas, a fim de salvaguardar a confidencialidade e a integridade dos dados que são transmitidos no contexto da comunicação entre os intervenientes.

Refira-se que esta comunicação se encontra sujeita ao ato delegado da Comissão Europeia, nomeadamente ao Regulamento Delegado (UE) 2018/389, que adota as normas técnicas de regulamentação e determina os requisitos aplicáveis às normas abertas de comunicação comuns e seguras a fim de garantir a segurança da comunicação entre os intervenientes. A eficácia e a segurança da comunicação são garantidas através do preenchimento dos requisitos em matéria de proteção e segurança dos dados bancários, definidos no Regulamento Delegado (UE) 2018/389, garantindo assim a interoperabilidade de diferentes soluções tecnológicas de comunicação[70].

3. Tratar os pedidos de dados ou as ordens de pagamento transmitidas através dos serviços do prestador dos serviços de pagamento.

Referimos antes que, de maneira a ser possível prestar o serviço de pagamento ao utilizador, o prestador do serviço tem, mediante uma ordem dada previamente, de solicitar acesso ao prestador de serviços de pagamento que gere a conta. Este acesso materializa-se através da (i) divulgação de dados bancários sobre contas de pagamento no caso do prestador do serviço de informação sobre contas; e (ii) no tratamento de ordens de pagamento, dadas pelo utilizador do serviço, no caso do prestador de iniciação de pagamentos.

O dever de tratar os pedidos de dados ou as ordens de pagamento deve ser realizado sem qualquer discriminação que não seja justificada por razões objetivas, nomeadamente em termos de prazos, de prioridade ou de encargos em relação às ordens de pagamento transmitidas diretamente pelo próprio ordenante.

2.4.2. DEVERES DO UTILIZADOR

utilizadores de serviços de pagamento dos prestadores de serviços de pagamento gestores de contas"

[70] Acrescenta o Considerando (93) da DSP 2 que *essas normas comuns e abertas deverão também garantir que o prestador do serviço de pagamento que gere a conta está ciente de que o contacto com ele estabelecido é efetuado por um prestador de serviços de iniciação de pagamentos ou por um prestador de serviços de informação sobre contas e não pelo próprio cliente. Essas normas comuns e abertas deverão também garantir que os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de informação sobre contas comuniquem de forma segura com o prestador do serviço de pagamento que gere a conta e com os clientes em causa*.

Ao abrigo do artigo 110º do RJSPME o utilizador dos serviços de pagamento está sujeito a duas principais obrigações associadas aos instrumentos, nomeadamente, (1) a utilização do instrumento de pagamento, nos termos das condições que regem a sua emissão e utilização, e ainda (2) a comunicação de perda, furto, roubo, apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento.

1. **Utilizar o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais;**

O dever de utilização do instrumento de pagamento, i. é., do serviço de iniciação do pagamento ou de informação sobre contas, obriga à utilização do mesmo de forma correta. O utilizador tem o dever de fazer uso do instrumento de pagamento, de acordo com as condições que regem a sua emissão e utilização e previamente acordadas entre as partes. Estas condições devem ser objetivas, não discriminatórias e proporcionais. Apesar de não se tratar de um dever principal sem sentido técnico-jurídico, é essencial para o bom funcionamento do serviço[71].

O n.º 2 do mesmo artigo acrescenta ainda que o utilizador deve tomar todas as medidas razoáveis para preservar a segurança das suas credenciais de segurança personalizadas. O utilizador deve ter a diligência de pautar sempre a sua conduta, no sentido de zelar pela proteção do instrumento de pagamento. Com este dever pretende-se que o utilizador não divulgue os seus dados pessoais e senhas de acesso a terceiros.

O motivo justificativo desta obrigação compreende-se, uma vez que toda a relação contratual e operações de pagamento realizadas nesse seguimento, estão acessíveis à distância por via eletrónica. Ora, não havendo necessidade de qualquer intervenção presencial do utilizador, a instituição não consegue tão facilmente aferir a identidade do ordenante. A solução encontrada para comprovar a legitimidade do ordenante, e garantir não se tratar de uma fraude, foi a disponibilização de senhas e códigos que apenas o mesmo tem conhecimento. Não divulgando as credencias de segurança a nenhum

[71] VERÓNICA SANTOS, "*As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de phishing e pharming. A questão da responsabilidade no âmbito das operações bancárias não autorizadas*." Dissertação de Mestrado, Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, 2018 p. 19.

terceiro, a instituição de crédito tem forma de comprovar que o ordenante corresponde à mesma pessoa que a parte contratual.

2. Comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento, alguma situação ilícita ou qualquer utilização não autorizada do instrumento de pagamento;

Ainda no âmbito das obrigações principais, o utilizador tem o dever de comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento[72].

Um dever essencial à realização de uma operação de pagamento é o consentimento, por parte do utilizador, da operação de pagamento. Para além da celebração dos contratos entre o utilizador e os prestadores de serviços de pagamento, é necessária uma aceitação expressa do utilizador na realização daquela determinada operação, sob pena de a execução da operação de pagamento não ser autorizada. A referida condição da autorização, como manifestação de vontade do utilizador, é exigida nos termos do artigo 103º do RJSPME, que determina no seu n.º 1 que a *operação de pagamento ou um conjunto de operações só se consideram autorizadas se o ordenante consentir*. O consentimento do utilizador apresenta-se, desta forma, como uma condição *sine quad non* para a autorização da execução da operação de pagamento. O consentimento deve ser dado previamente à realização da operação, com exceção de acordo em sentido diferente entre a utilizador do serviço e do prestador, e na forma acordada entre ambos.

Na prática o consentimento materializa-se, primeiramente, através do acesso ao API do prestador de serviços sobre contas ou de iniciação de pagamento, por parte do

[72] Neste âmbito chamamos a atenção para o Considerando (70) da DSP 2 que determina que "*A fim de reduzir os riscos e as consequências de operações de pagamento não autorizadas ou incorretamente executadas, o utilizador dos serviços de pagamento deverá informar o mais rapidamente possível o prestador desses serviços de quaisquer reclamações relativas a operações de pagamento alegadamente não autorizadas ou incorretamente executadas, desde que o prestador de serviços de pagamento tenha cumprido as suas obrigações de informação nos termos da presente diretiva. Se o prazo de notificação for cumprido pelo utilizador do serviço de pagamento, este deverá poder tramitar essas reclamações de acordo com os prazos nacionais de prescrição. A presente diretiva não deverá afetar outras reclamações entre utilizadores e prestadores de serviços de pagamento"*

utilizador. De seguida, o utilizador tem imprescindivelmente de inserir as suas credencias de segurança emitidas pela instituição de crédito – desde uma palavra-passe inventada pelo utilizador com determinadas características pelo prestador de serviços, ou de um código enviado por mensagem para o telemóvel ou mesmo de um número atribuído pelo prestador de serviços. São inúmeras as formas que o consentimento pode tomar. O que aqui importa chamar à colação é o facto de apenas o utilizador tenha conhecimento e acesso aos mesmos.

2.4.3. Deveres do Prestador de Serviços de pagamento complementar

A relação contratual que se estabelece entre o prestador de serviços e o utilizador, na maioria das vezes, constitui-se por via eletrónica, sem nunca haver uma necessidade de assinar presencialmente qualquer documento. Esta relação contratual estabelece-se somente através do recurso ao *smartphone*, mais precisamente do recurso à API do prestador de serviços.

O prestador de serviços de pagamento, seja ele de informação sobre contas ou de iniciação de pagamentos tem, igualmente, obrigações a que está sujeito, no âmbito da relação contratual com o utilizador, nos termos dos artigos 106º e 107º do RJSPME.

1. **Assegurar que as credenciais de segurança personalizadas do utilizador de serviços de pagamento não sejam acessíveis a terceiros, com exceção do utilizador e do emitente das credenciais de segurança personalizadas, e que sejam por si transmitidas através de canais seguros e eficientes;**

Um primeiro dever comum a ambos os prestadores de serviços de pagamento, ao abrigo dos artigos 106º, 3 b) e 107º, 2 b), é o dever de garantir que as credencias de segurança personalizadas do utilizador não sejam acessíveis a terceiros, mas apenas aos intervenientes. A exigência da segurança das credencias de segurança personalizadas justifica-se, pois são elementos personalizados fornecidos pelo prestador de serviços de pagamento a um utilizador de serviços de pagamento para efeitos de autenticação[73]. Falamos de dados de pagamento sensíveis, que podem ser utilizados para cometer fraudes, motivo pelo qual carecem de uma tutela especial. Nesta medida, cabe ao prestador de serviços de pagamento ser diligente e adotar todas os mecanismos

[73] Vide artigo 2º, j) do RJSPME.

necessários para impedir que as credenciais de segurança apenas sejam acessíveis ao utilizador.

É um verdadeiro dever especial de cuidado, que impende sobre o prestador de serviços de pagamento, em garantir a proteção da confidencialidade e integridade das credenciais e a segurança das mesmas, aquando da transmissão, que deve ser realizada através de canais seguros e eficientes. Justifica-se este dever, uma vez que os serviços de pagamento fornecidos através da Internet ou de outros canais à distância, cujo funcionamento não depende do local onde estão fisicamente situados o dispositivo utilizado para iniciar a operação de pagamento ou o instrumento de pagamento utilizado, devem incluir a autenticação do utilizador que inclua elementos que associem de forma dinâmica a operação a um montante e beneficiário específicos, de modo a que o utilizador se encontre sempre informado do que está a autorizar[74]. A utilização segura de credenciais de segurança personalizadas é, desta forma, necessária para limitar os riscos de atividades fraudulentas.

As credenciais de segurança personalizadas[75] são utilizadas para a autenticação segura do cliente pelo utilizador do serviço de pagamento. A autenticação forte do cliente traduz-se, desta forma, num mecanismo que permita garantir ao prestador de serviços de pagamento a identidade do ordenante da transação em questão ou a validade da utilização de um instrumento de pagamento específico, utilizando para isso, no mínimo dois elementos característicos da própria pessoa.

O instituto da autenticação forte surge com a entrada em vigor da DSP 2 e revela a relevância atribuída, pelo legislador europeu, à segurança das operações de pagamento e à proteção dos clientes contra riscos de fraude. Assim, uma operação de pagamento que seja realizada remotamente, para que o prestador do serviço consiga identificar o

[74] Preâmbulo do RJSPME.
[75] Vide Considerando (30) da DSP 2 que refere que *os prestadores de serviços de iniciação de pagamentos não estabelecem necessariamente uma relação contratual com os prestadores de serviços de pagamento que gerem as contas e, independentemente do modelo de negócio utilizado pelos prestadores de serviços de iniciação de pagamentos, os prestadores de serviços de pagamento que gerem as contas deverão possibilitar que os prestadores de serviços de iniciação de pagamentos se baseiem nos procedimentos de autenticação facultados pelos prestadores de serviços de pagamento que gerem as contas para iniciarem um pagamento específico em nome do ordenante.*

ordenante e a validade da utilização do instrumento de pagamento, pressupõe que seja exigida a autenticação forte do cliente.

2. **Identificar-se junto do prestador de serviços de pagamento que gere a conta e comunicar de forma segura com o prestador de serviços de pagamento que gere a conta e com o utilizador de serviços de pagamento;**

Outro dever comum aos prestadores de serviços de iniciação de pagamentos e de serviços de informação sobre contas é o de identificação do próprio junto da instituição de crédito, assim como o de comunicação segura. A identificação do prestador de serviço complementar junto do prestador de serviços de pagamento que gere a conta permite verificar a identidade do prestador do serviço.

A identificação[76] do prestador de serviços de pagamento é mecanismo utilizado pelo prestador de serviços que gere a conta para verificar se aquele prestador reúne todos requisitos necessários e em que medida é adequado dar acesso aos serviços de pagamentos de forma eficiente e sem entraves. Permite, assim, ao prestador de serviços de pagamento gestor de contas verificar, à *priori*, a idoneidade daquele prestador de serviços.

É, desta forma, um mecanismo de proteção do prestador de serviços de pagamento que gere a conta, pois permite que este verifique, num primeiro momento, a identidade da entidade a quem vai dar acesso a informação do seu cliente.

3. **Não utilizar nem armazenar dados, nem aceder aos mesmos para outros fins que não sejam a prestação do serviço de iniciação do pagamento expressamente solicitado pelo ordenante;**

Atendendo ao disposto nos artigos 106º, alínea g) e 107º, alínea f) identificamos um dever comum aos novos prestadores de serviços, nomeadamente o de proibição de utilização e armazenamento de dados para fins diversos aos da prestação do serviço previamente estabelecido entre as partes. Numa perspetiva de proteção adequada dos dados e das contas de pagamento do utilizador do serviço, devem os prestadores utilizar

[76] Regulada pelo Regulamento Delegado (UE) 2018/389 da Comissão de 27 de novembro de 2017 que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho.

a informação a que têm acesso, estritamente no contexto da prestação do serviço de pagamento e da ordem dada pelo utilizador.

Novamente estamos perante um dever que evidencia a componente da segurança da cadeia de pagamentos e da falta de proteção dos consumidores em determinados domínios, na medida em que impõe uma proibição de utilização dos dados e um armazenamento diverso ao estabelecido.

Tendo em conta a sensibilidade desses dados, importa dizer a este respeito, que os novos prestadores de serviços não se encontram atualmente abrangidos pelo RGICSF, que regula o acesso à atividade e respetivo exercício por parte das instituições de crédito e das sociedades financeiras e o exercício da supervisão das instituições de crédito e das sociedades financeiras, os respetivos poderes e instrumentos. Estes serviços e prestadores de serviços estão apenas sujeitos ao disposto na DSP 2 e no ordenamento jurídico português ao RJSPME, o que pode levantar muitas questões jurídicas designadamente em matéria de supervisão da atividade desenvolvida. Mais adiante aprofundaremos o tema.

4. Não armazenar dados de pagamento sensíveis do utilizador de serviços de pagamento (iniciação de pagamento), nem exige dados de pagamento sensíveis associados às contas de pagamento (informação sobre contas);

Atendendo ao disposto no artigo 2º, k), dados de pagamentos sensíveis definem-se como dados, incluindo credenciais de segurança personalizadas, que podem ser utilizados para cometer fraudes, não constituindo dados de pagamento sensíveis, no âmbito das atividades dos prestadores do serviço de iniciação do pagamento e dos prestadores de serviços de informação sobre contas, o nome do titular da conta e o número da conta.

Os dados de pagamento sensíveis permitem ao prestador do serviço identificar o utilizador e verificar se é aquela a pessoa com quem contratou, permitindo igualmente ao utilizador de efetuar a autenticação, seja a nível de uma operação de pagamento, seja para aceder às suas contas de pagamento em linha. Ao proibir o armazenamento e a proibição de exigência de acesso a este tipo de dados, o legislador procurou manter, de forma mais exclusiva possível, o acesso à informação do utilizador o mais exclusivo possível.

5. **Assegura que quaisquer outras informações sobre o utilizador de serviços de pagamento, obtidas aquando da prestação do serviço de iniciação do pagamento, sejam prestadas exclusivamente ao beneficiário, e apenas com o consentimento expresso do utilizador de serviços de pagamento (iniciação de pagamentos) e presta serviços exclusivamente com base no consentimento expresso do utilizador de serviços de pagamento (informação sobre contas);**

Se atentarmos ao disposto nos artigos 106º, n.º 3, c) verificamos que outro dever que incumbe aos prestadores de serviços de pagamento é assegurar que a informação sobre o utilizador de serviços de pagamento, obtidas pelo prestador de serviços de iniciação de pagamento, sejam prestadas exclusivamente ao beneficiário. A divulgação de informação sobre o utilizador ao beneficiário pode justificar-se, na medida em que é interveniente na operação de pagamento em causa.

A intenção do legislador foi de garantir que a informação sobre o utilizador fornecida pelo prestador do serviço, em especial informações de carácter pessoal, é somente acessível ao beneficiário enquanto terceiro na relação contratual com a entidade bancária e/ou com o prestador do serviço. Tratando-se de uma pessoa fora do âmbito dessa relação contratual e que, desta forma, não se encontra sujeito ao dever de sigilo, justifica o dever de manter a segurança da informação e o prevenir assim o perigo da informação em causa não ser alvo de fraude informática.

Deverão, neste sentido, ser adotadas as medidas e diligências que estejam ao seu alcance para que a informação seja exclusivamente divulgada ao beneficiário. Impende sobre o prestador do serviço um especial dever de cuidado no momento em que é partilhada a informação, devendo a mesma ser transmitida através de canais seguros e eficientes.

O instituto do consentimento, previsto no artigo 103º do RJSPME e no artigo 64º da DSP 2, desempenha um papel essencial no âmbito dos serviços de pagamento. Se compararmos a previsão do consentimento da DSP 2 com o do RJSPME, percebemos que, na sua íntegra, são semelhantes, na medida em que determinam que a operação de pagamento só é considerada autorizada se o ordenante tiver dado o seu consentimento à execução da operação de pagamento.

O consentimento deve ser concedido previamente à execução da operação, salvo acordo em sentido contrário e deve ser dado na forma acordada entre o ordenante e o prestador de serviços de pagamento. Conforme refere a DSP 2 o consentimento para executar uma operação de pagamento também pode ser concedido através do beneficiário ou do prestador de serviços de iniciação de pagamentos, e não obrigatoriamente pelo ordenante[77].

Também no âmbito da relação entre o utilizador e o prestador de serviços de informação sobre contas, cada operação realizada carece, previamente, de uma manifestação de vontade no sentido de realização dessa mesma operação, por ambas as partes. Estas terão de ter concordado na execução da ordem dada. Todos e quaisquer serviços prestados devem partir de um consentimento dado pelo utilizador.

Novamente assistimos a uma manifestação de um dos principais pilares da DSP 2 – a segurança. Neste caso em concreto, trata-se da segurança (ou risco de insegurança) dos pagamentos eletrónicos. O desenvolvimento tecnológico, o aperfeiçoamento da técnica dos pagamentos eletrónicos e o aumento, à escala global, do consumo deste tipo de serviços obrigou à adaptação, a nível legislativo, em matéria de direitos e obrigações relacionados com a prestação e utilização de serviços de pagamento [78].

Deveres como os que acabámos de expor são exatamente espelho disso. Trata-se de mecanismos que servem para mitigar a eventual realização de operações fraudulentas.

6. Não exigir ao utilizador de serviços de pagamento quaisquer outros dados além dos necessários para prestar o serviço (iniciação de pagamento), e aceder exclusivamente às informações das contas de pagamento designadas e das operações de pagamento associadas (informação sobre contas);

Da mesma maneira que o prestador do serviço de iniciação de pagamentos não deve aceder a dados que extravasem o âmbito do estritamente necessário à prestação do

[77] *Vide* artigo 64º, 2º da DSP 2.
[78] Considerando (7) da DSP 2 *Nos últimos anos, assistiu-se a um aumento dos riscos de segurança relacionados com os pagamentos eletrónicos. Isto deve-se à maior complexidade técnica dos pagamentos eletrónicos, ao volume cada vez maior deste tipo de pagamentos à escala mundial e ao aparecimento de novos tipos de serviços de pagamento. A existência de serviços de pagamento seguros constitui uma condição indispensável para o bom funcionamento do mercado de serviços de pagamento. Os utilizadores de serviços de pagamento deverão ser, pois, protegidos de forma adequada contra esses riscos. Os serviços de pagamento são essenciais para o funcionamento de atividades económicas e sociais da máxima importância.*

serviço, o prestador de serviços sobre informação sobre contas apenas acede a informação associada às contas de pagamento em questão e às respetivas operações de pagamento. O legislador procurou impor limites ao acesso à informação do utilizador, por parte dos prestadores de serviços, e, desta forma, zelar pela proteção e segurança dos dados.

Na relação entre a instituição de crédito e o cliente, este último goza de uma proteção acrescida, na medida em que a instituição de crédito está sujeita ao RGICSF, seguindo assim regras mais rígidas em matéria de deveres de conduta e diligência (artigos 74º e 75º do diploma), assim como ao disposto na Diretiva 2007/64/CE sobre serviços de pagamento no mercado interno.

Ao invés do que acontece na relação entre o utilizador e o prestador de serviços de pagamento complementares, a relação com a instituição de crédito é pautada por deveres de diligência e conduta (artigos 74º e 75º do RGICSF), entre outros[79]. Por seu turno, na relação com os prestadores de serviços de pagamento complementares, o utilizador está mais desprotegido, o que justifica o dever limitativo sobre os dados do utilizador.

De seguida, e para concluir este capítulo, estudaremos dois deveres que impendem exclusivamente sobre cada um dos prestadores de serviços de pagamento, em função da natureza do serviço que prestam.

7. Não deter em momento algum dos fundos do ordenante no âmbito da prestação do serviço de iniciação do pagamento;

Os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de informação sobre contas, quando prestam exclusivamente esses serviços, têm acesso aos fundos, mas não detêm fundos dos clientes. Apesar de disporem de acesso à

[79] Com efeito "(...) *deveres de lealdade, deveres de alerta, aviso, advertência e prevenção para certos riscos e a sua repartição, deveres de informação esclarecimento e conselho, deveres de descrição e sigilo profissional, cuja inobservância ou violação poderá por em causa a uberrina fides do cliente e o institutus personae da relação e assim originar a responsabilidade da instituição financeira não criteriosa e ordenada na sua conduta leal de promoção e respeito consciencioso dos interesses que lhe estão confiado"*, JOÃO CALVÃO SILVA, "Serviços de pagamento e responsabilidade civil", in: Estudos em homenagem a Rui Manchete, Coimbra, Almedina, 2015.

informação bancária desses mesmos fundos, a lei impõe que estes prestadores não detenham nem movimentem os fundos dos mesmos.

Este dever vem apenas previsto no âmbito da prestação de serviços de iniciação de pagamento – o que faz sentido, atendendo à natureza do serviço. Neste serviço de pagamento, o prestador do mesmo apenas tem a função de consultar a informação bancária sobre uma ou mais contas de pagamento detidas pelo utilizador. A competência do prestador do serviço cinge-se à verificação e agregação dos saldos e posterior disposição dos mesmos ao utilizador. O prestador do serviço não tem competência para aceder, gerir e realizar movimentos aos fundos do utilizador.

Refere a DSP 2 que deverão ser tomadas medidas para manter os fundos do utilizador do serviço de pagamento separados dos fundos da instituição de pagamento. São necessários requisitos de salvaguarda quando uma instituição de pagamento estiver na posse de fundos do utilizador do serviço de pagamento. Caso a mesma instituição de pagamento execute uma operação de pagamento tanto para o ordenante como para o beneficiário e seja concedida uma linha de crédito ao ordenante, poderá ser adequado salvaguardar os fundos a favor do beneficiário, uma vez que representam o crédito do beneficiário perante a instituição de pagamento. As instituições de pagamento deverão estar igualmente sujeitas a requisitos eficazes em matéria de combate ao branqueamento de capitais e ao financiamento do terrorismo[80].

No entanto, é importante que possam cumprir as suas responsabilidades em relação às atividades que exercem, pelo que deverão obrigatoriamente subscrever um seguro de responsabilidade civil profissional ou garantia equivalente.

8. Não altera o montante, o ordenante nem qualquer outro elemento da operação.

Por último, mas não menos importante, o prestador de serviços de iniciação de pagamentos não tem a liberdade para, unilateralmente, alterar qualquer elemento da ordem dada pelo utilizador. Seja a nível do montante da ordem de pagamento, o próprio ordenante, entre outros.

[80] *Vide* Considerando (37) da DSP 2.

3) DOS DADOS PESSOAIS

Nas palavras do Professor ANTÓNIO MENEZES CORDEIRO[81] o *Direito bancário é um Direito de informações.* O mesmo autor continua que *no Direito bancário, em face da perfeita predeterminação dos intervenientes – banqueiros e cliente – e tendo em conta o valor das operações e a necessidade extrema da precisão, as informações redobram de valor e assumem um papel pioneiro, em termos de regulação. Digamos que no Direito bancário, as informações há muito perderam a sua natureza instrumental e secundária: antes surgem como objeto principal de muitas obrigações*[82]. A atividade bancária assenta na realização de operações bancárias que *pressupõem a identificação e a constante comunicação das correspondentes posições ativas ou passivas, o que tem que ser realizado através da prestação de informações, exigindo, por isso a atividade bancária uma permanente recolha e circulação de informação*[83]. Desta forma, os bancos dispõem hoje em dia, mais do que qualquer entidade, de um grau de informação muito elevado dos seus clientes, que versa tanto, sobre a esfera pública (nome, idade, género) e a esfera privada, como a esfera íntima do sujeito.

No momento em que são disponibilizados os dados pessoais a instituição de crédito fica encarregue de recolher, tratar e armazenar os dados do cliente, que depois são utilizados para os mais variados fins, desde comerciais, publicitários, de controlo de risco, entre outros[84].

A eventualidade de a entidade bancária partilhar os dados bancários do cliente com uma instituição de pagamento levanta questões aos mais variados níveis, designadamente em matérias de proteção dos consumidores, de segurança e de responsabilidade, bem

[81] ANTÓNIO MENEZES CORDEIRO, *Direito Bancário*, 6ª ed. rev. e atualizada, Almedina, 2016, pp. 403.
[82] No mesmo sentido, LUÍS MANUEL TELES DE MENEZES LEITÃO, *Informação bancária e responsabilidade,* in estudos em homenagem ao Prof. Doutor Inocêncio Galvão Telles / org. António Menezes Cordeiro, Luís Menezes Leitão, Januário Costa Gomes, Almedina, Vol. 2, 2002, p. 225.
[83] LUÍS MANUEL TELES DE MENEZES LEITÃO, *Informação bancária e responsabilidade*, in estudos em homenagem ao Prof. Doutor Inocêncio Galvão Telles / org. António Menezes Cordeiro, Luís Menezes Leitão, Januário Costa Gomes, Almedina, Vol. 2, 2002, p. 225.
[84] NELSON RICARDO GOUVEIA PEREIRA ROCHA, *A proteção dos dados do cliente bancário na cessão de crédito em incumprimento*, Dissertação de Mestrado, Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, p. 17, 2016

como em matérias de concorrência e de dados bancários, especialmente no que ao tratamento e à proteção de dados pessoais diz respeito.

Com isto em mente, a DSP 2[85] reconhece que a prestação de serviços de pagamento implica o tratamento de dados pessoais[86] e refere que os seguintes diplomas são aplicáveis ao tratamento de dados pessoais para efeitos da presente Diretiva, sendo eles a Diretiva 95/46/CE[87], entretanto revogada pelo RGPD, e o Regulamento (CE) n. 45/2001[88], também revogado pelo Regulamento (UE) 2018/1725[89]. Apesar da referência aos referidos diplomas estar desatualizada, a mesma justifica-se pelo facto a entrada em vigor do RGPD ter sido posterior ao processo legislativo da DSP 2. Fazendo uma interpretação atualista da remissão, podemos concluir que o disposto no RGPD é aplicável à prestação de serviços de pagamento. O mesmo considerando avança ainda que no tratamento de dados deverão ser respeitados os princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período proporcionado de conservação de dados, reforçando o direito à proteção de dados pessoais.

[85] Pode ler-se no Considerando 89 que *a prestação de serviços de pagamento pelos prestadores de serviços de pagamento pode implicar o tratamento de dados pessoais. A Diretiva 95/46/CE do Parlamento Europeu e do Conselho (1), as regras nacionais que transpõem a Diretiva 95/46/CE e o Regulamento (CE) n. 45/2001 do Parlamento Europeu e do Conselho ( ) são aplicáveis ao tratamento de dados pessoais para efeitos da presente diretiva. Em especial, caso os dados pessoais sejam tratados para efeitos da presente diretiva, deverá ser especificado o objetivo exato, deverá ser referida a base jurídica aplicável, deverão ser cumpridos os requisitos de segurança aplicáveis estabelecidos na Diretiva 95/46/CE e deverão ser respeitados os princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período proporcionado de conservação de dados. De igual modo, a proteção de dados desde a conceção e a proteção de dados por defeito deverão estar incorporadas em todos os sistemas de tratamento de dados desenvolvidos e utilizados no quadro da presente diretiva.*

[86] Já anteriormente a DSP 1 fazia, apesar de muito sinteticamente. O artigo 79º da DSP 1: *Os Estados-Membros permitem o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento caso tal se revele necessário para salvaguardar a prevenção, a investigação e a deteção de fraudes em matéria de pagamentos. O tratamento desses dados pessoais deve ser realizado nos termos da Diretiva 95/46/CE.*

[87] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[88] Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados.

[89] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados.

3.1. ENQUADRAMENTO DOS DADOS BANCÁRIOS ENQUANTO DADOS PESSOAIS

Para procedermos ao enquadramento dos dados bancários enquanto dados pessoais cumpre, num primeiro momento, averiguar o âmbito de aplicação material e territorial do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (adiante designado por "RGPD") à operação bancária aberta.

Nos termos da alínea a) do artigo 4.º do RGPD dados pessoais definem-se como a *informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular*. A alínea b) do mesmo artigo refere ainda que o tratamento de dados pessoais se considera *uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.*

O RGPD encarrega-se de disponibilizar uma definição clara do conceito de dados pessoais, permitindo identificar o seu âmbito, assim como de especificar a forma de operar os dados pessoais. O RGPD prevê ainda um conjunto de princípios gerais relativos ao tratamento dos dados pessoais, no seu artigo 5.º, sendo que chamamos à atenção para o princípio previsto no n.º 1 desse artigo, segundo o qual o tratamento deve ser *lícito, leal e transparente em relação ao titular dos dados*.

De facto, parte dos dados que são disponibilizados pelo cliente à entidade bancária são suscetíveis de ser considerados *informação relativa a uma pessoa singular identificada ou identificável* ("dados pessoais"). Na verdade, no momento da celebração

do contrato de abertura de conta, o titular dos dados é obrigado a ceder uma série de dados, que incluem *nome, número de identificação, dados de localização, identificadores por via eletrónica* e, pelo menos, *elementos específicos da identidade económica*, tornando-o uma pessoa singular identificável. Contudo, não é de descurar que o âmbito da definição de dados pessoais é consideravelmente mais abrangente, não sendo grande parte dos dados que a entidade bancária dispõe do cliente suscetíveis de serem considerados *elementos específicos da identidade física, fisiológica, genética, mental, cultural ou social dessa pessoa singular*. Ainda assim, pelo acima exposto, tudo leva a crer que os dados bancários são considerados uma categoria de dados pessoais.

Ademais, sobre a aplicação material do RGPD dispõe o n.º 1 do artigo 2.º que o mesmo se aplica *ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados*. O n.º 2 do mesmo artigo, por sua vez, discrimina uma série de situações específicas, no âmbito das quais o diploma não é aplicável, entre as quais a atividade económico-financeira. Face ao disposto no artigo 2.º do diploma tudo indica que o RGPD de aplica materialmente à atividade levada a cabo tanto por uma instituição de crédito como uma instituição de pagamento. Da mesma maneira não se afigura a não aplicação territorialmente do RGPD, sendo que o mesmo se aplica *ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União*[90].

Por fim, relevante a este propósito é o artigo 94º da DSP 2 que refere que *o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento* [é permitido] *quando tal for necessário para salvaguardar a prevenção, a investigação e a deteção de fraudes em matéria de pagamentos*. Mais uma vez, a DSP 2 remete, no mesmo artigo, para a Diretiva 95/46/CE, revogada pelo RGPD, e defende que a informação das pessoas sobre o tratamento de dados pessoais e sobre qualquer outro tratamento de dados pessoais para efeitos da presente Diretiva é efetuada nos termos desse diploma. O n.º 2 da mesma norma restringe o acesso aos dados pessoais ao necessário

[90] N.º 1 do artigo 3.º do RGPD.

para a prestação dos serviços de pagamento, assim como o tratamento e conservação, sempre com o consentimento expresso do utilizador de serviços de pagamento.

3.2. DA AUTENTICAÇÃO FORTE DO CLIENTE

Já referimos anteriormente que os novos serviços de pagamento complementares não estão atualmente abrangidos pelo RGICSF, pelo que não são necessariamente supervisionados por uma autoridade competente, nem estão obrigados a cumprir as regras definidas nesse mesmo diploma. A falta de um conjunto de condições de segurança na execução das operações e de uma supervisão adequada pode provocar uma desproteção dos consumidores, de segurança e de responsabilidade, bem como em matéria de concorrência e de proteção de dados, especialmente no que respeita à proteção dos dados do utilizador de serviços de pagamento em conformidade com as regras da União em matéria de proteção de dados.

O motivo apresentado pela DSP 2 para esta, a nosso ver, simples sujeição dos prestadores dos serviços de pagamento apenas à DSP 2 e ao seu pacote legislativo e regulamentar é o facto de serem entidades que não detêm fundos dos clientes[91]. Nos termos da DSP 2 será desproporcionado impôr requisitos de fundos próprios a estes novos operadores de mercado[92].

O artigo 13º da DSP 1 definia que os Estados-Membros era onerados do dever de possuir um registo público das instituições de pagamento autorizadas e respetivos agentes e sucursais, das pessoas singulares e coletivas e respetivos agentes e sucursais, que estivessem habilitadas nos termos da legislação nacional a prestar serviços de pagamento, de maneira a identificar os serviços de pagamento para os quais a instituição de pagamento tenha sido autorizada ou a pessoa singular ou coletiva se encontre registada. Graças à evolução tecnológica e do próprio mercado a DSP 2, por sua vez, foi mais longe e encarregou a EBA de elaborar e gerir um registo central no qual publique uma lista de firmas das entidades que prestam serviços de pagamento[93].

[91] Referimo-nos a prestadores que efetivamente prestarem exclusivamente esses serviços.
[92] Vide Considerando (35) da DSP 2.
[93] Vide artigo 15º da DSP 2.

O regime protecionista dos utilizadores dos serviços trata-se de uma matéria que se manifesta igualmente através do Regulamento Delegado (UE) 2018/389. De modo a assegurar a segurança e transparência a DSP 2 encarregou a EBA de elaborar orientações e projetos de normas técnicas de regulamentação sobre questões de segurança dos serviços de pagamento, designadamente no que respeita à autenticação forte do cliente, em matéria de comunicação aberta entre as entidades intervenientes, bem como sobre a cooperação entre Estados-Membros no contexto da prestação de serviços e do estabelecimento de instituições de pagamento autorizadas noutros Estados-Membros. O Regulamento Delegado (UE) 2018/389 veio complementar o pacote legislativo e regulamentar associado à DSP 2 e regular as normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras.

Na perspetiva de que os serviços de pagamento oferecidos por via eletrónica devem ser prestados de forma segura, adotando tecnologias suscetíveis de garantir a autenticação segura do utilizador e de reduzir, tanto quanto possível, o risco de fraude, surge a autenticação forte do cliente. Sempre que os prestadores de serviços de pagamento apliquem a autenticação forte do cliente nos termos do n.º 1 do artigo 97.º da DSP 2, a autenticação deve basear-se na utilização de dois ou mais elementos pertencentes às categorias de conhecimento, posse e inerência, sendo estes independentes entre eles[94].

A autenticação forte do cliente exige que para conceder a autorização de uma operação de pagamento, o utilizador deve inserir dois ou mais elementos pertencentes às categorias de conhecimento (algo que só o utilizador conhece), como a extensão ou a complexidade, para os elementos pertencentes à categoria da posse (algo que só o utilizador possui), como especificações algorítmicas, o comprimento da chave e a entropia informacional, e para os dispositivos e software que leiam elementos pertencentes à categoria da inerência (algo que o utilizador é), como especificações algorítmicas, características de proteção baseada em sensores biométricos e modelos, nomeadamente para reduzir o risco de estes elementos serem descobertos, divulgados junto de partes não autorizadas e por elas utilizados. É ainda necessário estabelecer requisitos que assegurem a independência destes elementos, de modo a que a violação de um deles não comprometa a fiabilidade dos restantes, em especial quando um destes elementos seja utilizado através de um dispositivo multifuncional, como um tablet ou um

[94] N.º 30 do artigo 4º da DSP 2.

telemóvel, suscetível de ser utilizado tanto para dar a instrução de realização do pagamento como no processo de autenticação[9596]. O código de autenticação só deve ser aceite uma vez pelo prestador de serviços de pagamento quando o ordenante o utilizar para aceder em linha à sua conta de pagamento, iniciar uma operação de pagamento eletrónico ou realizar uma ação, através de um canal remoto, suscetível de envolver um risco de fraude no pagamento ou outros abusos.

O artigo 97º da DSP 2 e o artigo 104º do RJSPME preveem três situações nas quais os prestadores de serviços de pagamento devem aplicar a autenticação forte do cliente, a saber (i) caso o ordenante aceda em linha à sua conta de pagamento; (ii) caso o ordenante inicie uma operação de pagamento eletrónico; ou (iii) caso o ordenante realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou de outros abusos. Temos, desta forma, a previsão da autenticação forte no caso do serviço de informação sobre contas e no serviço de iniciação do pagamento. O último cenário previsto pelo legislador foi, a nosso ver, definido intencionalmente em termos muito gerais para permitir abranger um maior número de situações de fraude e de forma a acautelar situações fraudulentas que surjam no futuro em face da sucessiva evolução tenológica.

Tanto o legislador europeu como o legislador nacional vão mais longe no caso do serviço de iniciação de pagamento e acrescentam que nestes casos o prestador do serviço deve adotar uma autenticação forte do cliente que inclua elementos que associem de forma dinâmica a operação a um montante específico e beneficiário específicos. Já no caso do serviço de informação sobre contas de pagamento, o legislador europeu oferece a possibilidade de os prestadores de serviços de informação sobre contas de pagamento poderem não aplicar a autenticação forte do cliente[97], sob condição de cumprimento dos requisitos definidos no n.º 2 do mesmo artigo.

Por fim, importa também acrescentar que a instituição de crédito permite que o prestador do serviço de iniciação do pagamento e o prestador de serviços de informação sobre contas se baseiem nos procedimentos de autenticação facultados pela instituição de crédito.

[95] Considerando (6) do Regulamento Delegado (UE) 2018/389.
[96] Artigo 2º, d) do RJSPME.
[97] N.º 1 do Artigo 10º do Regulamento Delegado (UE) 2018/389.

4) DA RESPONSABILIDADE

Depois de analisadas as vantagens e os benefícios da operação bancária aberta, em especial a celeridade e a comodidade destes dois novos tipos de serviços, interessa agora proceder à análise das fragilidades do sistema[98]. A realidade problemática sobre a qual estamos a tentar refletir resulta da sensibilidade dos dados pessoais dos clientes e do facto de os mesmos serem partilhados entre entidades. Para melhor entendermos esta fragilidade, cumpre recapitular o motivo desta ameaça.

No caso do serviço do serviço de informação sobre contas, na medida em que o utilizador acede a uma interface para consultar os saldos das suas contas de pagamento de forma agregada, a disponibilização destes valores pressupõe a consulta prévia de informação sobre uma ou mais contas de pagamento detidas pelo utilizador, junto de uma ou mais instituições de crédito por parte do prestador de serviços. Para que a disponibilização de informações agregadas em linha sobre uma ou mais contas de pagamento seja possível, o prestador do serviço teve, de antemão, de ter acesso às mesmas através de interfaces em linha dos prestadores de serviços de pagamento que gerem as contas. Já no caso do serviço de iniciação de pagamentos, que não detenha fundos do utilizador em nenhuma fase da cadeia de pagamentos, sendo o objetivo deste serviço assegurar ao beneficiário do pagamento, que o pagamento seja realizado, de maneira a que este disponibilize o bem ou preste o seu serviço, para o prestador do serviço do pagamento, processa-se a transferência de informações através interface de acesso que permita uma comunicação segura, estando os intervenientes nesta partilha sujeito ao risco de perda, extravio ou adulteração dos dados bancários por terceiros.

De todo o modo, há um ponto em comum em ambos os serviços: um sujeito cliente de uma instituição de crédito recorre a um serviço de pagamento complementar, que por sua vez carece de aceder a determinados dados pessoais sensíveis detidos pela instituição

[98] Toda a atividade bancária realizada pressupõe permanentes comunicações entre os intervenientes e tem subjacente uma constante recolha e circulação de informação. No âmbito da operação bancária aberta o valor das informações assume uma importância ainda maior, uma vez que, como já vimos anteriormente, requer a disponibilização dessa mesma informação bancária a uma entidade terceira à relação jurídica entre a instituição de crédito e o seu cliente. Desta forma, a informação bancária assume um papel fulcral, na prestação do serviço do serviço de informação sobre contas ou no serviço de iniciação de pagamentos, motivo pelo qual a instituição de crédito deve cumprir determinados deveres e pautar as suas condutas de acordo com obrigações muito rigorosas.

de crédito. Perante o consentimento do cliente, a instituição de crédito disponibiliza os dados ao prestador do serviço, de maneira a conseguir prestar o serviço de pagamento.

Apesar do esforço de eliminação das debilidades potenciadas pela facilidade do alcance, pelo anonimato e pela automaticidade da *internet*, situações de fraude são difíceis de prever e podem significar grandes riscos, perigos e vulnerabilidades para todos os seus intervenientes.

Um primeiro momento passa pela prevenção de operações de fraude e da utilização abusiva dos dados, através do cumprimento rigoroso dos deveres de cada interveniente, anteriormente elencados. Quando falhada a referida prevenção, a abordagem a ter constitui a determinação de quem (e em que medida) são suportados os prejuízos decorrentes das operações lesivas. Num segundo momento pós-prevenção impõe-se que seja apurada a responsabilidade e quem (e em que termos) deve suportar os prejuízos causados por aquelas atividades.

Ocupar-nos-emos do mecanismo de defesa do cliente bancário/utilizador do serviço de pagamento em caso de perda, extravio ou adulteração dos dados bancários e, eventual, fraude informática, da análise do ónus da prova, e dos deveres que impendem sobre as partes. Procuraremos analisar em que exato momento e em função de que conduta dos intervenientes recai a responsabilidade no processo de recolha, arquivo, utilização e transmissão dos dados pessoais dos seus clientes. Para tal, partiremos da análise da fonte formal direta – a lei aplicável a estas situações – e faremos referência a fontes formais indiretas – a jurisprudência.

4.1. Da Responsabilidade por perda, extravio ou adulteração dos dados bancários

A DSP 2 reconhece[99] que a prestação de serviços de pagamento pelos prestadores de serviços de pagamento pode implicar o tratamento de dados pessoais. Referimos, anteriormente que pela sensibilidade dos dados bancários que são transferidos, entre entidades, mediante as APIs, os deveres e obrigações das partes são muito rigorosos. Numa situação de perda, extravio ou adulteração dos dados bancários que possibilite a abertura de uma brecha na segurança, aumentando assim o risco de ocorrência de uma

[99] Vide Considerando (89) da DSP 2.

fraude informática por parte de um terceiro. No âmbito da operação bancária aberta, o paradigma das fragilidades, riscos, perigos e vulnerabilidades resulta da necessidade de partilha e armazenamento de dados pessoais entre os agentes económicos que, pela sensibilidade da informação bancária, pode resultar em práticas mais lesivas ao utilizador do serviço, nomeadamente operações de *phishing* e/ou *pharming*. Partindo do pressuposto que o cliente/utilizador não intervém no processo de partilha dos dados entre a instituição de crédito e o prestador do serviço de pagamento complementar, à exceção da ordem de execução inicial, a responsabilidade recairá sobre uma das duas entidades. Neste ponto interessa determinar o momento exato em que a responsabilização se transmite de um interveniente para o outro.

4.2. DA RESPONSABILIDADE POR OPERAÇÕES BANCÁRIAS NÃO AUTORIZADAS

Conforme escreve FRANCISCO MENDES CORREIA quando uma operação não tenha sido executada por parte do banco, e o utilizador e titular da conta invoque que a mesma não foi previamente por si autorizada, podem isolar-se quatro constelações prototípicas de factos subjacentes: a operação foi realmente autorizada pelo utilizador (a) ou, pelo contrário, a operação não foi autorizada e sua realização fica a dever-se a factos imputáveis a título de culpa ao banco (b), ao utilizador (c) ou a terceiro (d)[100].

Refira-se que para efeitos deste estudo, focaremos a nossa análise em situações em que a operação não tenha sido efetivamente autorizada pelo utilizador e a sua execução fique a dever-se a factos imputáveis a um terceiro fraudulento, ficando o prestador obrigado a repor o estado da conta em que estava antes da operação e/ou ao prestador a título censurável, por incumprimento de deveres ou omissão de atos a que estava sujeito. A situação que pretendemos analisar conjuga, desta forma, a constelação (b) e (d) do parágrafo anterior.

Numa eventual situação em que aquando da partilha de dados bancários ocorra a perda, extravio ou adulteração dos mesmos, provocando assim a abertura de uma brecha na segurança do sistema e que permita a penetração e o acesso de terceiros aos dados bancários confiados tanto à instituição de crédito como ao prestador do serviço de pagamento complementar, surge a possibilidade de sucederem prejuízos decorrentes de

[100] CORREIA, Francisco Mendes, *Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica*, in: Revista de Direito Civil, 2017, p. 708.

operações não autorizadas. Antes de mais, deixamos claro que neste ponto não estamos perante uma situação de verdadeira imputação da responsabilidade, mas sim de repartição dos prejuízos, uma vez que, a quem deve ser realmente imputada a responsabilidade é ao terceiro que realiza a operação de pagamento não autorizada[101].

4.2.1. À LUZ DO DIREITO COMUM

Parafraseando o Professor Luís Menezes Leitão *a prestação de informações apresenta-se como uma das obrigações essenciais no âmbito da relação duradoura, uma vez que o cliente tem de confiar nos registos das operações bancárias que efetua para todo o momento as poder documentar [...]. No entanto esta atividade de recolha e difusão de informação essencial ao funcionamento do sistema bancário, é uma atividade que pode ser igualmente lesiva [...]*.

Neste ponto focaremos a nossa análise nas soluções apresentadas pelo Direito comum do instituto da responsabilidade contratual[102], recorrendo ao artigo 796º do CC. Note-se que a prestação de informações num quadro contratual pressupõe naturalmente a prévia celebração do contrato relativo à prestação de informação por parte do banco, pelo que os pedidos do cliente relativos a certas informações não são vinculativos para o mesmo, sendo que este as pode prestar ou não [...][103]. Tivemos oportunidade anteriormente de explorar a relação contratual entre o cliente bancário e a instituição de crédito, assim como a possibilidade de recusa por parte do banco prevista no n.º 2 do artigo 69º da DSP 2.

Nos termos do artigo 796º do CC n*os contratos que importem a transferência do domínio sobre certa coisa ou que constituam ou transfiram um direito real sobre ela, o perecimento ou deterioração da coisa por causa não imputável ao alienante corre por conta do adquirente.* Desta norma resulta que é sobre a instituição de crédito que impende o ónus de elidir a presunção legal, demonstrando para o efeito a culpa do prestador do

[101] RAQUEL SOFIA RIBEIRO DE LIMA, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa*, Dissertação de Mestrado em Direito pela Faculdade de Direito da Universidade do Porto, 2016, 35.
[102] Excluímos a responsabilidade delitual por entendermos não se aplicar o artigo 485º do CC.
[103] LEITÃO, Luís Menezes, "*Informação bancária e Responsabilidade"*, em Estudos Galvão Telles 2, 2002, p. 228.

serviço na falta de restituição dos prejuízos em caso de perdas resultantes dos ataques de fraude informática[104].

Também neste sentido o STJ proferiu[105] que *através do ato de depósito o tradens aceita transferir para a esfera de domínio (propriedade) do accipiens o risco sobre a gestão da quantia que transferiu, sendo que a partir desse momento se alheia da responsabilidade quanto ao uso e fruição, por transferência para a esfera de responsabilidade do depositário. Cabe ao depositário, enquanto proprietário da coisa transferida, responder pelo risco de extravio ou dissipação da coisa até ao montante exigível no momento da solicitação da restituição.*

Noutra situação[106], o mesmo Tribunal entendeu que *os riscos da falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta dos bancos, do aqui Réu portanto, por a tal conduzir o disposto no artigo 796º, nº1 do CCivil, não se tendo provado, como não se provou, que tivesse havido culpa da Autora* (aqui cliente bancário).

Não podemos ignorar também que no âmbito desta atividade profissional *os administradores e os empregados das instituições de crédito devem proceder, tanto nas relações com os clientes como nas relações com outras instituições, com diligência, neutralidade, lealdade e discrição e respeito consciencioso dos interesses que lhes estão confiados*[107], concretizando o mesmo diploma que *membros dos órgãos de administração das instituições de crédito, bem como as pessoas que nelas exerçam cargos de direção, gerência, chefia ou similares, devem proceder nas suas funções com a diligência de um gestor criterioso e ordenado, de acordo com o princípio da repartição de riscos e da segurança das aplicações e ter em conta o interesse dos depositantes, dos investidores, dos demais credores e de todos os clientes em geral*[108]. Também aqui encontramos

---

[104] VERÓNICA SANTOS, "*As debilidades do serviço de homebanking …",* acrescenta que *o risco inerente à conta do cliente, o risco relacionado com a obrigação de restituir coisa do mesmo género e qualidade, não pode deixar de correr por conta do banqueiro,* Dissertação de Mestrado, Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, 2018.
[105] Ac. STJ, de 07-10-2010, com o relator Serra Baptista, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/7e6e904d4d57102c802577b500560396?OpenDocument
[106] Ac. STJ de 18-12-2013, com o relator Ana Paula Boularot, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/0feb7fef778a3b6780257c46003d2073?OpenDocument&Highlight=0,6479%2F09
[107] Artigo 74º do RGICSF.
[108] Artigo 75º do RGICSF.

indícios de que se pressupõe uma diligência qualificada, designadamente que a atividade bancária seja desenvolvida com elevados níveis de competência técnica[109] e praticada por um gestor criterioso e ordenado, de acordo com o princípio da repartição de riscos e segurança das aplicações[110]. A este respeito refere JOÃO CALVÃO DA SILVA tratar-se de *um "bónus argentarius", portanto, a quem a lei impõe especiais deveres de proteção dos clientes contra riscos operacionais de deficiências e fraudes associados a à prestação dos serviços de levantamentos, pagamentos ou transferências eletrónicos, como riscos próprios da indústria financeira cujos custos devem ser disseminados por todos os potenciais utilizadores para potenciar a confiança no seu uso generalizado, no interesse de todos, das instituições de pagamento, dos empresários, dos comerciantes e dos consumidores*[111].

Pelo exposto e acreditando que a instituição de crédito está numa melhor posição para precaver situações de risco de operações não autorizadas, consideramos que à luz do Direito comum o risco corre por conta da instituição de crédito. Trata-se de um tema que diverge opiniões, sendo que alguns não consideram aplicar-se o artigo 796º do CC.

4.2.2. À LUZ DA SEGUNDA DIRETIVA DE SERVIÇOS DE PAGAMENTO

As operações não autorizadas surgem habitualmente (embora não necessariamente) da inobservância dos deveres que recaem sobre os intervenientes, i.e., quando um dos operadores omite atos devidos ou pratique atos que configurem o incumprimento ou o incumprimento defeituoso das suas obrigações, sendo que pode acontecer que mesmo que as obrigações sejam devidamente cumpridas, se verifiquem operações de pagamento não autorizadas por factos imputáveis a um terceiro fraudulento, não existindo juízo de ilicitude nestes casos. Partiremos do cenário que temos vindo a imaginar ao longo deste texto, designadamente de um terceiro com intenções fraudulentas identificar uma brecha na segurança do sistema – seja ela derivada da perda, extravio ou adulteração dos dados bancários provoca pelo terceiro ou por negligência do cumprimento rigoroso dos deveres que impendem sobre a instituição de crédito e/ou prestador do serviço complementar.

[109] Artigo 73º do RGICSF.
[110] Artigo 75º do RGICSF.
[111] JOÃO CALVÃO SILVA, *Serviços de pagamento e responsabilidade civil*, in: Estudos em homenagem a Rui Manchete, Almedina, 2015, p. 355.

O artigo 114º do RJSPME determina que o prestador de serviços de pagamento do ordenante *deve reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada após ter tido conhecimento da operação ou após esta lhe ter sido comunicada e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação*[112]. Como sugere o Professor FRANCISCO MENDES CORREIA esta norma *apenas enumera os direitos invocáveis pelo utilizador (reembolso da conta e reposição da situação atual hipotética), e que pressupõe que a realização da operação, por não ter sido autorizada pelo utilizador, pode ser imputada ao prestador, a título censurável*.

Ainda no âmbito desta disposição ressalvamos a importância da notificação por parte do cliente/utilizador[113] a dar conhecimento à instituição de crédito da ocorrência de determinada operação que não foi por si autorizada. O ato de notificar a instituição de consagra um momento-chave a partir do qual surge na esfera do banco um dever de bloquear[114] o instrumento de pagamento e impedir a sua posterior utilização.

No contexto da relação contratual existente entre o cliente bancário e a instituição de crédito insere-se o dever geral de correção desta última que se traduz numa especial obrigação de proteção dos interesses dos clientes através da adoção de instrumentos idóneos à prevenção e eliminação de áleas operacionais típicas associadas à atividade de prestação de serviços, designadamente serviços informáticos, automáticos, eletrónicos e à distância[115].

---

[112] O n.º 2 do mesmo artigo estabelece que o prestador de serviços de pagamento do ordenante não está obrigado ao reembolso no prazo previsto no número anterior se tiver motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e comunicar por escrito esses motivos, no prazo indicado no número anterior, às autoridades judiciárias nos termos da lei penal e de processo penal.

[113] Dever de comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento, alguma situação ilícita ou qualquer utilização não autorizada do instrumento de pagamento previsto na alínea b) do n.º 1 do artigo 110º do RJSPME.

[114] Alínea e) do n.º 1 do artigo 111.º.

[115] JOÃO CALVÃO SILVA, *Serviços de pagamento e responsabilidade civil*, in: Estudos em homenagem a Rui Manchete, Almedina, 2015, p. 352.

O RJSPME prevê igualmente as situações em que a operação de pagamento foi iniciada através de um prestador do serviço de iniciação do pagamento[116], situações em que a instituição de crédito deve reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada após ter tido conhecimento da operação ou após esta lhe ter sido comunicada e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação, não sendo o reembolso devido em situações que o prestador do serviço de iniciação do pagamento lhe dê conhecimento de que tem motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e de que comunicou por escrito esses motivos às autoridades judiciárias nos termos da lei penal e de processo penal.

A posição tomada pela DSP 2 e consequentemente pelo RJSPME face à imputação da responsabilidade ao prestador do serviço de pagamento complementar foi sempre no sentido de delimitar a mesma[117] atendendo ao facto de prestarem exclusivamente esses serviços, não deterem fundos dos clientes[118]. O motivo que o legislador europeu apresenta é o facto de afigurar ser desproporcionado impor requisitos de fundos próprios a estes novos operadores de mercado e o facto de estas exercerem atividades mais especializadas e limitadas, que acarretam, por conseguinte, riscos mais reduzidos e mais fáceis de

[116] Neste sentido, refere o Considerando 86 da DSP 2 que *o prestador do serviço de pagamento do ordenante, a saber, o prestador de serviços de pagamento que gere a conta ou, se for caso disso, o prestador do serviço de iniciação do pagamento, deverá assumir a responsabilidade pela execução correta do pagamento, em especial no tocante à totalidade do montante da operação de pagamento e ao prazo de execução, e a plena responsabilidade por qualquer falha das outras partes na cadeia de pagamentos, até à conta do beneficiário. Em consequência desta responsabilidade, se a totalidade do montante não for creditada ao prestador do serviço de pagamento do beneficiário ou se for creditada com atraso, o prestador do serviço de pagamento do ordenante deverá retificar a operação de pagamento ou, sem demora indevida, reembolsar ao ordenante o montante correspondente dessa operação, sem prejuízo de quaisquer outros pedidos de reembolso que possam ser apresentados nos termos do direito nacional. Em virtude da responsabilidade do prestador do serviço de pagamento, nem o ordenante nem o beneficiário deverão suportar quaisquer custos relacionados com a execução incorreta do pagamento. Em caso de não execução, de falhas na execução ou de execução tardia das operações de pagamento, os Estados-Membros deverão garantir que a data-valor das operações de retificação do pagamento realizadas pelos prestadores de serviços de pagamento corresponde sempre à data-valor aplicável em caso de execução correta.*

[117] Pode ler-se no Considerando (74) da DSP 2 que *no caso dos serviços de iniciação de pagamentos, os direitos e as obrigações dos utilizadores de serviços de pagamento e dos prestadores de serviços de pagamento intervenientes deverão ser adequados aos serviços prestados. Mais especificamente, a repartição de responsabilidades entre o prestador do serviço de pagamento que gere a conta e o prestador do serviço de iniciação do pagamento que intervém na operação deverá obrigá-los a assumir a responsabilidade pelas partes respetivas da operação sob o seu controlo.*

[118] É objeto da presente Dissertação apenas este tipo de prestadores de serviços.

acompanhar e controlar do que os inerentes ao leque mais vasto de atividades das instituições de crédito.

4.3. DO ÓNUS DA PROVA

Numa situação de litígio, a determinação de qual dos intervenientes recai o ónus da prova, i. é., em que momento e qual dos intervenientes deve provar que a operação de pagamento foi realizada corretamente, consubstancia um exercício fulcral da resolução. A eventual situação de litígio a que nos referimos pode assumir diferentes hipóteses. Pode o litígio ter origem na prestação deficiente, insuficiente ou errónea à outra parte, resultando, desta forma, de uma atuação que lhe seja imputável ou que incumpra as obrigações e deveres impostos ou pode o litígio surgir por força da realização de uma operação sem a devida autorização, fruto de um esquema de fraude informática, nomeadamente o *phishing* ou o *pharming*, situações essas que envolvem um terceiro que praticou o crime.

Analisemos primeiramente o regime geral. Dispõe o n.º 1 do artigo 342.º do CC que *àquele que invocar um direito cabe fazer a prova dos factos constitutivos do direito alegado*. As regras gerais definem que quem invoque o direito deve provar os factos constitutivos, i. é., pertencendo à instituição de crédito o dever de informação, deve o cliente bancário provar a sua insipiência dos factos e o conhecimento por parte da instituição e do prestador do serviço de pagamento complementar.

Atendendo ao regime jurídico estatuído no RJSPME, caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada ou alegue que a operação não foi corretamente efetuada, cabe à instituição de crédito *fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento*[119]. O RJSPME abrange igualmente o prestador do serviço de iniciação do pagamento no âmbito de aplicação continuando no n.º 2 do mesmo artigo que *se a operação de pagamento tiver sido iniciada através de um prestador do serviço de iniciação do pagamento, recai sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada*

[119] N.º 1 do artigo 113º do RJSPME.

e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado.

O mesmo preceito acrescenta ainda que *caso um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, a utilização do instrumento de pagamento registada pelo prestador de serviços de pagamento, incluindo o prestador do serviço de iniciação do pagamento, se for caso disso, não é necessariamente suficiente, por si só, para provar que a operação de pagamento foi autorizada pelo ordenante, que este último agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira.* Para se exonerar do dever de reembolsar o valor dos prejuízos, a instituição de crédito incluindo, se for caso disso, o prestador do serviço de iniciação do pagamento, deve apresentar elementos que demonstrem a existência de fraude, de dolo ou de negligência grosseira da parte do utilizador de serviços de pagamento. Terá assim de ser provado o grau de participação do cliente bancário/utilizador na operação de pagamento em causa, bem como o grau de culpa.

Neste sentido, refere VERÓNICA SANTOS[120] que *a presunção de culpa que recai sobre o Banco deve-se ao facto de não pode ser alocado ao utilizador o ónus de um sistema que ele não domina, sistema este informaticamente bastante complexo, estando por isso o prestador de serviços em melhor posição de evitar o risco de operação não autorizada pelo cliente.*

Como podemos comprovar o ónus da prova pertence ao respetivo prestador do serviço de pagamento – seja o prestador uma instituição de crédito, seja um prestador do serviço de iniciação do pagamento. É à instituição de crédito que recai o dever de provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência e que o comportamento negligente do titular e a medida em que esse contribuiu para as operações não autorizadas[121]. Determina o RJSPME que incumbe igualmente ao prestador do serviço de iniciação do pagamento o ónus de provar que a operação foi realizada

[120] VERÓNICA SANTOS, "*As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de phishing e pharming. A questão da responsabilidade no âmbito das operações bancárias não autorizadas*." Dissertação de Mestrado, Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, 2018 p. 39.
[121] RAQUEL SOFIA RIBEIRO DE LIMA, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa*, Dissertação de Mestrado em Direito pela Faculdade de Direito da Universidade do Porto, 2016.

corretamente. Chamamos à atenção para o facto do legislador europeu, no caso de o prestador de iniciação do pagamento referir especificamente que o ónus da prova apenas recai sobre este, no âmbito da sua esfera de competências[122], ao invés do n.º 1 (que abrange as instituições de crédito) em que oculta o âmbito do ónus.

Trata-se de um desvio em comparação ao regime geral que anteriormente analisámos. A solução apresentada pelo RJSPME apresenta-se mais favorável ao utilizador do que a regra geral. Em suma, em matéria de ónus de prova, tanto a instituição de crédito como o prestador de serviços de iniciação de pagamentos estão onerados com um ónus da prova nas suas competências. Caberá tanto a um como ao outro fazer a prova dos factos constitutivos do direito alegado.

4.4. DO REEMBOLSO DO MONTANTE EM CASO DE OPERAÇÕES DE PAGAMENTO NÃO AUTORIZADAS

Na sequência de uma operação de pagamento não autorizada, o utilizador de serviços de pagamento com direito a utilizar um instrumento de pagamento deve comunicar, logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento[123].

Nos termos do n.º 1 do artigo 113º, realizada a comunicação e caso o utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.

O RJSPME prevê ainda uma consequência civil a situação de o ordenante não ser imediatamente reembolsado pelo prestador de serviços de pagamento, e não terem havido motivos razoáveis que constituam fundamento válido de suspeita de fraude, ou essa suspeita não tenha sido comunicada, por escrito. Como tutela do utilizador o RJSPME

[122] Vide Considerando (74) da DSP 2.
[123] Alínea b), n.º 1 do artigo 110º.

determina que são devidos ao ordenante juros moratórios, contados dia a dia desde a data em que o utilizador de serviços de pagamento tenha negado que autorizou a operação de pagamento executada, até à data do reembolso efetivo da mesma, calculados à taxa legal, fixada nos termos do CC, acrescida de 10 pontos percentuais, sem prejuízo do direito à indemnização suplementar a que haja lugar.

Ainda no âmbito do artigo 114.º avança a mesma norma que caso a operação de pagamento seja iniciada através de um prestador do serviço de iniciação do pagamento, a instituição de crédito deve reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada após ter tido conhecimento da operação ou após esta lhe ter sido comunicada e, em todo o caso, o mais tardar até ao final do primeiro dia útil seguinte àquele conhecimento ou comunicação. Neste caso, a tutela atribuída pelo Regime recai sobre o ordenante, ao invés do utilizador.

Contudo, o dever do reembolso imediato não se mantém, caso o prestador do serviço de iniciação do pagamento lhe der conhecimento de que tem motivos razoáveis para suspeitar de atuação fraudulenta do ordenante e de que comunicou por escrito esses motivos às autoridades judiciárias nos termos da lei penal e de processo penal. Se, porventura, o prestador do serviço de iniciação de pagamento for responsável pela operação de pagamento não autorizada, o RJSPME prevê que este último deve indemnizar imediatamente a instituição de pagamento, a pedido deste, pelos danos sofridos ou pelos montantes pagos em resultado do reembolso ao ordenante, incluindo o montante da operação de pagamento não autorizada[124].

Da leitura que fazemos deste regime, podemos mais uma vez identificar uma manifestação da garantia do elevado nível de proteção dos consumidores. De facto, temos vindo a evidenciar que esta foi uma das principais bandeiras da DSP 2 e consequentemente do RJSPME, motivo pelo qual os ordenantes deverão ter sempre o direito de dirigir o seu pedido de reembolso ao prestador de serviços de pagamento que gere a sua conta, mesmo em caso de intervenção de um prestador de serviços de iniciação de pagamentos na operação de pagamento. Esta disposição, contudo, não prejudica a repartição de responsabilidades entre os prestadores de serviços de pagamento.

[124] N.º 8 do artigo 114.º do RJSPME.

5) CONCLUSÃO

Ao longo desta dissertação temos vindo a realçar a vertente inovadora e recente dos novos serviços de pagamento e do importantíssimo papel desempenhado pela tecnologia financeira e como tal veio revolucionar o modelo bancário tradicional. Não podemos, nesta medida, iniciar esta conclusão sem abordar o tema das novas tecnologias financeiras como eventual ameaça à indústria financeira já anteriormente consolidada. Serão estas novas tendências um impulso e um incentivo para os incumbentes se inovarem?

A pergunta que se procura responder é: são as *Fintech* disruptivas para o sistema financeiro ou vieram antes acrescentar e complementar o mesmo? Serão elas disruptivas se, por um lado, concorrerem com as grandes instituições bancárias, provocando uma larga preferência do novo serviço de pagamento pelo utilizador face ao modelo tradicional, e por serão estas complementares se, por outro lado, contribuírem como novo elemento?

Como refere a Professora Madalena Perestrelo de Oliveira *para que uma tecnologia seja considerada disruptiva não basta que seja inovadora. [...] Para merecer esta qualificação a inovação tem de ser caracterizada pela (i) capacidade de mudança; (ii) pelo potencial substitutivo; e (iii) pelo impacto estrutural*[125]. Por outras palavras, a inovação é disruptiva quando a empresa que oferecer o novo negócio, assumindo uma dimensão consideravelmente mais pequena face às empresas concorrentes, consegue desafiar o modelo de negócio tradicional ao ponto de provocar uma alteração estrutural no setor.

As novas tecnologias forçam os incumbentes a adaptarem-se ao novo modelo de negócio, sob pena de verem o seu número de clientes reduzido por opção pelo inovador e moderno modelo de negócio. O cliente torna-se mais exigente e sofisticado, com expetativas mais elevadas, ficando insatisfeito com um serviço arcaico.

[125] MADALENA PERESTRELO DE OLIVEIRA, *As recentes tendências da Fintech: disruptivas e colaborativas*, in FinTech - Desafios da Tecnologia Financeira, Vol. 1, 2ª ed., Almedina, 2019, pp. 71-81.

Após um longo "ciclo de sofrimento"[126][127], que percorre os diferentes estados de reações das instituições de crédito à intervenção das tecnologias *fintech*, esse mesmo percurso termina com uma fase de aceitação. Uma aceitação de que a convergência entre a tecnologia e os serviços financeiros é inevitável e que perfaz o novo normal[128]. Nesta fase, as instituições financeiras reconhecem as vantagens da adoção de novas tecnologias à prestação dos serviços[129]. A cooperação entre incumbentes e os novos intervenientes torna-se uma oportunidade e satisfaz as necessidades de ambas as partes.

O *Basel Committee on Banking Supervision*, num relatório elaborado em fevereiro de 2018 elenca as variadas vantagens diretas. Uma primeira vantagem é a inclusão financeira. Apenas seis em cada dez adultos detêm uma conta bancária, embora existam mais dispositivos móveis do que pessoas no mundo. O investimento nos serviços digitais permitiu o acesso aos serviços financeiros por cada vez mais pessoais, podendo a tecnologia chegar a locais remotos. Os serviços financeiros podem ser prestados a mais pessoas com maior rapidez, responsabilidade e eficiência.

Um benefício igualmente a ter em conta é o aperfeiçoamento e personalização dos serviços bancários. As empresas *fintech* podem ajudar as instituições financeiras a aperfeiçoar os seus serviços tradicionais através de uma oferta mais personalizada com

---

[126] Do inglês *grief cycle*.

[127] Para mais desenvolvimentos sobre o "ciclo de sofrimento", disponível no sítio: https://jpnicols.com/2016/07/12/fintech-grief-cycle-bankers/

[128] Basel Committee on Banking Supervision, *Sound Practices Implications of fintech developments for banks and bank supervisors*, 2018, disponível em: https://www.bis.org/bcbs/publ/d431.pdf

[129] No mesmo sentido, LAURA BRODSKY e LIZ OAKES, *Data sharing and open banking*, artigo da Mckinsey & Company, 2017, referem que *embora pareça inevitável que a operação bancária aberta resulte no sacrifício de algum grau de controlo por parte das instituições de crédito já estabelecidas, estas também obterão o benefício compensatório de participar em maiores profit pools, nas quais deverão estar bem posicionadas para desempenhar um papel de liderança: por exemplo, criar novas propostas de serviços que combinem análises preditivas, inteligência artificial, e financiamento para melhorar as ofertas aos consumidores e às empresas. Entre os incumbentes, a vantagem de ser o primeiro a ser escolhido está aberta a organizações proactivas e suficientemente ágeis para serem os primeiros a fornecer produtos inovadores e apelativos que os clientes desejam e necessitam (por exemplo, interfaces intuitivas e serviços de valor acrescentado tais como orçamentação, categorização de despesas tais como as oferecidas por operadores digitais como Monzo). O estatuto de "agente de confiança" de que gozam atualmente os incumbentes estabelecidos continuará a ser uma vantagem competitiva durante algum tempo, mas deve ser explorado agora para travar a perda de negócios para os novos prestadores de serviços*, disponível no sítio: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

recurso a *white label robo advisors* que permitam ajudar os clientes ter uma experiência melhor e mais personalizada.

Os baixos custos de transação e os serviços bancários mais céleres são igualmente uma grande vantagem destas tecnologias. As inovações dos agentes *fintech* podem acelerar as transferências e os pagamentos e reduzir os seus custos, especialmente em transferências transfronteiriças, no caso das quais as empresas *fintech* podem, em alguns casos, fornecer serviços bancários mais rápidos a custos mais baixos.

A intervenção das tecnologias *fintech* oferece um processo bancário melhorado e mais eficiente. A inovação pode permitir a realização de operações num ambiente mais seguro graças à utilização de tecnologias criptográficas ou biométricas e de sistemas mais interoperáveis, diminuindo as hipóteses de falha.

O potencial impacto positivo na estabilidade financeira devido ao aumento da concorrência é também apontado pelo *Basel Committee on Banking Supervisio*n como uma vantagem. A entrada de novos intervenientes em concorrência com instituições financeiras estabelecidas, pode eventualmente fragmentar o mercado de serviços financeiros e reduzir o risco sistémico associado aos intervenientes de dimensão sistémica.

Por fim o surgimento da *Regtech* assume também uma importante vantagem. A *fintech* pode ser utilizada para melhorar os processos de *compliance* nas instituições financeiras. A criação de regulamentação continua a aumentar a nível mundial, e o desenvolvimento e aplicação eficazes da "regtech" pode criar oportunidades no sentido de, por exemplo, proporcionar a criação de relatórios automatizados.

Afiguram-se como numerosas as vantagens de comodidade, celeridade e de baico custo que a operação bancária aberta oferece ao utilizador destes serviços de pagamento. A aliança entre a instituição de crédito e o prestador de serviços complementar, que seja bem-sucedida, complementa as desvantagens/ fragilidades de cada uma das partes. Por um lado, obriga as instituições de crédito a inovarem os serviços que apresentam aos seus clientes, e por outro, introduz os prestadores de serviços à base de clientes bancários existentes. No entanto, a desmaterialização da realidade negocial financeira, fruto da evolução tecnológica, vem acompanhada de uma preocupação com a insegurança digital.

Neste âmbito, sugerem-se três grandes vetores que devem ser acautelados[130], são eles (i) desenvolver mecanismos *standard* que permitam a interação facilitada entre instituições de crédito e *third-party providers*[131]; (ii) estabelecer soluções adequadas aos ecossistemas para maximizar a segurança e minimizar a exposição dos utilizadores à fraude informática[132]; e (iii) proporcionar clareza e consistência na forma de gerir investigações, assim como na resolução de litígios[133].

Se de facto a partilha da quota de mercado entre instituições de crédito e instituições de pagamento se afigura como uma grande vantagem por contribuir para alavancar a concorrência e a eficiência na prestação de serviços de pagamento, também é certo que acarreta um grande risco – a insegurança na partilha de dados bancários. No âmbito da operação bancária aberta, o paradigma das fragilidades, riscos, perigos e vulnerabilidades resulta da necessidade de partilha e armazenamento de dados pessoais entre os agentes económicos, que pela sensibilidade da informação bancária, pode resultar em práticas mais lesivas ao utilizador do serviço, nomeadamente operações de *phishing* e/ou *pharming*. As operações lesivas para o cliente resultantes da perda, extravio ou

---

[130] MASTERCARD, *Delivering on the promises of Open Banking*, Artigo técnico elaborado em colaboração com a Ovum, 2019, disponível em: https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/white-paper-delivering-promises-open-banking.pdf

[131] Segundo o mesmo artigo a *fragmentação das normas API continua a ser um obstáculo potencial para a adoção de serviços de operação bancária aberta. Enquanto a indústria estão a trabalhar para resolver este problema, os serviços third-party providers na Europa continuam hoje em dia a ser, em grande parte, prestadores de serviços de informação de contas, utilizando APIs encomendadas. A passagem para serviços de iniciação de pagamentos exigirá alguma forma de normalização sobre a formatação de dados na indústria, bem como uma Autenticação Forte do Cliente, normas API harmonizadas (mesmo para APIs comerciais) e uma experiência de desenvolvimento suave.*

[132] Sobre este ponto, explica o artigo que *outra preocupação chave entre a indústria relaciona-se com a segurança dos dados bancários dos clientes. A proteção dos participantes no ecossistema da operação bancária aberta contra terceiros com índole criminosa desempenhará um papel muito importante na construção da confiança em novos serviços. Para as instituições de crédito, a eventualidade de uma fraude é uma preocupação significativa, especialmente referente ao prestador do serviço de iniciação de pagamentos. Como comenta Andrew Churchill, Consultor de Segurança e Investigador em Estratégia Tecnológica, comenta: "As instituições de crédito foram efetivamente pressionadas no sentido de embarcarem em ações que implicam risco, e com possíveis perdas de clientes e receita - é a sua reputação que pode ficar em risco. Se uma third-party provider é alvo de fraude, a instituição de crédito é responsável - o que parece agradar a Comissão Europeia".*

[133] Sobre este ponto o artigo refere que *antes da operação bancária aberta, havia um número quase ilimitado de formas através das quais os clientes podiam precisar do apoio do seu banco para resolver algum tipo de problema, quer com outra parte (como um comerciante), quer com o próprio banco. Consequentemente, desenvolveram-se mecanismos claros para o conseguir, sendo os manuais em torno das transações com cartões de pagamento um exemplo particularmente bom de como gerir os potenciais desafios que surgem entre múltiplos intervenientes. Acrescentar prestadores de serviços de pagamento complementares aumenta drasticamente o desafio. De facto, a forte possibilidade de um litígio envolver um cliente, pelo menos uma instituição de crédito, um prestador de serviços de pagamento complementar e um terceiro, tal como um comerciante, demonstra uma clara necessidade de uma forma de centralização do processo de resolução.*

adulteração dos dados bancários são habitualmente fruto, embora não necessariamente, da inobservância das obrigações que recaem sobre as partes envolventes. Pode, naturalmente, suceder-se uma situação de fraude informática, através do acesso online de um terceiro, mediante a utilização de programas informáticos para o efeito ou a usurpação de mecanismos de segurança, obtendo assim o acesso aos dados do cliente e, realizando, desta forma, transferências de fundos sem o consentimento do titular da conta.

A importância da proteção e segurança deste bem jurídico é evidente na leitura da DSP 2[134], que procura sempre implementar normas e princípios que minimizem a probabilidade de violação do mesmo e consagrar uma quantidade de deveres e obrigações que determinem as condutas corretas dos intervenientes. O acesso indevido a estes dados bancários pode consubstanciar-se em ataques informáticos e intromissão não autorizada por terceiros fraudulentos nas contas de pagamento ou da realização de uma operação de pagamento não autorizada.

No seio da responsabilidade por operações bancárias não autorizadas a solução apresentada pelo quadro legal foi no sentido de limitar a responsabilidade ao prestador do serviço de pagamento complementar, em prejuízo da responsabilidade pela instituição bancária. Refira-se que em matéria de ónus da prova, tanto a instituição de crédito como o prestador de serviços de iniciação de pagamentos estão onerados com um ónus da prova no âmbito das suas competências.

Por fim, se por um lado as operações de pagamento realizadas através de meios eletrónicos são incontornáveis no cumprimento quotidiano das obrigações pecuniárias de particulares e/ou empresa, por outro, acreditamos que sendo a convergência entre a tecnologia e os serviços de pagamento – em especial o surgimento e reconhecimento legal dos serviços de iniciação do pagamento e o de informação sobre contas – um acontecimento muito jovem, gozou até agora de pouco tempo para se manifestar e para ser trabalhado nos nossos Tribunais. Na prática, os contratos-quadro e as operações de pagamento por eles abrangidas são de longe mais comuns e importantes de um ponto de vista económico do que as operações de pagamento de caráter isolado. Apesar das

[134] Determina o Considerando (28) da DSP 2 que os *serviços deverão ser igualmente abrangidos pela presente diretiva, de modo a que os consumidores disponham de proteção adequada para os dados relativos ao pagamento e à conta, bem como de certeza jurídica quanto ao estatuto de prestador de serviços de informação sobre contas.*

decisões jurisprudenciais existentes, grande parte delas reconduz-se ao serviço do *homebanking* e ao *pharming* e *phishing* associados a esse instrumento de pagamento. Acreditamos tratar-se de uma realidade que embora assuma expressão ainda diminuta em Portugal, conta com tem todo o potencial para integrar os hábitos das operações de pagamento.

ÍNDICE BIBLIOGRÁFICO

- ALMEIDA, Carlos Ferreira de "*Contrato Bancário Geral e Depósito Bancário*", Coleção de Formação Continua – Direito Bancário, Lisboa: Centro de Estudos Judiciários (2015), disponível em: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf

- AUTORIDADE DA CONCORRÊNCIA, "*Inovação Tecnológica e Concorrência no Sector Financeiro em Portugal"*, Issues Paper, 2018, disponível em: http://www.concorrencia.pt/vPT/Estudos_e_Publicacoes/Estudos_Economicos/Banca_e_Seguros/Documents/Versão%20Final%20Issues%20Paper%20FinTech.pdf

- BARBER, Andrew, *Open banking will facilitate home loan switching*, artigo para a Pinsent Masons, 2017, disponível em: https://www.pinsentmasons.com/out-law/news/uk-moving-from-open-banking-to-open-finance

- BARBOSA, Mafalda Miranda, "*Serviços de pagamentos, repartição do risco e responsabilidade civil: algumas reflexões a propósito da nova diretiva dos serviços de pagamentos (DSP2)"*, in: Revista de Direito Comercial, Edição 2017

- BASEL COMMITTEE ON BANKING SUPERVISION, *Sound Practices Implications of fintech developments for banks and bank supervisors*, 2018, disponível em: https://www.bis.org/bcbs/publ/d431.pdf

- BRODSKY, Laura e OAKES, Liz, *Data sharing and open banking*, artigo pela McKinsey & Company 2017, disponível em: https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking

- CORDEIRO, António Menezes, Direito bancário, 6ª ed. rev. E atualizada, Almedina, 2016

- CORDEIRO, António Menezes, *Litigância de má fé, abuso do direito de ação e culpa in agendo*, n.º 33, 2005

- CORREIA, Francisco Mendes, *Operações não autorizadas e o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica*, in: Revista de Direito Civil. - Lisboa, 2015-. - A. 2, nº 3, 2017

- CORREIA, Francisco Mendes, "*Uma revolução permanente? A DSP 2 e o novo Direito dos Serviços de Pagamento*", in III Congresso de direito bancário, Coimbra, 2017, p. 385-404

- DUARTE, Diogo Pereira, "*Response to the Commission consultation paper on Fintech: a more competitive and innovative financial sector",* in: Revista de direito das sociedades, A. 9, nº 3 (2017), Coimbra, 2009

- FinTech, RegTech and the Reconceptualization of Financial Regulation, Northwestern Journal of International Law & Business, Forthcoming, University of Hong Kong Faculty of Law Research Paper No. 2016/035

- GUIMARÃES, Maria Raquel, *A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (home banking): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09*, in: Cadernos de Direito Privado, CEJUR, No. 41, 2013

- GUIMARÃES, Maria Raquel, *Os contratos quadros de prestação de serviços de pagamento*, in: I Congresso de direito do consumo, Almedina, 2016. - p. 177-188.

- GUIMARÃES, Maria Raquel, *(Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento eletrónicos em operações presenciais e à distância : análise do regime introduzido pelo Anexo I do Decreto-Lei n.º 317/2009, de 30 de Outubro (RSP), e das alterações que se perspetivam face à Proposta de Directiva do Parlamento Europeu e do Conselho, de 24 de Julho de 2013*, in: I Congresso de Direito Bancário, Almedina, 2015

- GUIMARÃES, Maria Raquel, *O phishing de dados bancários e o pharming de contas: análise jurisprudencial*, in: III Congresso de direito bancário Almedina, 2018. - p. 405-432

- LEITÃO, Luís Menezes, *Informação bancária e Responsabilidade*, em Estudos Galvão Telles 2, 2002

- LIMA, Sofia Ribeiro de, *A responsabilidade pela utilização abusiva on-line de instrumentos de pagamento eletrónico na jurisprudência portuguesa*; Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto, 2016;

- MAGNUSON, William, *Regulating Fintech*, Vanderbilt Law Review, Forthcoming, Texas A&M University School of Law Legal Studies Research Paper No. 17-55, 2017

- MASTERCARD, *Delivering on the promises of Open Banking*, Artigo técnico elaborado em colaboração com a Ovum, 2019, disponível em: https://www.mastercard.us/content/dam/public/mastercardcom/na/us/en/documents/white-paper-delivering-promises-open-banking.pdf

- MIRANDA, Sérgio Manuel Basto Cândido Sedoura de, *O Segredo Bancário e a Administração Tributária*, Trabalho Final no III Curso de Pós-Graduação em Direito Fiscal, 2007

- MOREIRA, Tiago Correia, *Partilha de dados pessoais e operação bancária aberta*, in: FinTech - Desafios da Tecnologia Financeira, Vol. 2., 1ª ed., Almedina, 2019

- MOURA, Carlos, *FinTech e regulação no mercado bancário*, in: FinTech - Desafios da Tecnologia Financeira, Vol. 1, 2ª ed., Almedina, 2019

- NAVARETTI, Giorgio Barba, "*Fintech and Banking. Friends or Foes?"*, European Economy, Banks, Regulation and the Real Sector, 2017

- PALHÃO, Bruno Silva, *Os serviços de pagamento e as operações não autorizadas*, in: Cadernos de Direito Privado, n.65, 2019, p.3-17

- BASTO, Inês Caria Pinto, *A nova Diretiva de Serviços de Pagamento*, Actualidad Jurídica Uría Menéndez, Madrid, n.46 (2017), p.118-123

- PEREIRA, Tiago da Cunha, "*DSP 2: Oportunidades e Desafios"*, in: Revista de Direito Financeiro e dos Mercados de Capital, Vol. 1, No. 5, 2019

- ROCHA, Nelson Ricardo Gouveia Pereira, "*A proteção dos dados do cliente bancário na cessão de crédito em incumprimento*"; Dissertação de Mestrado, Faculdade de Direito da Universidade de Lisboa 2016;

- RODRIGUES, Maria João, "*Depósito bancário",* in: Cadernos O Direito, Temas de Direito Bancário, N.º 9, Almedina, 2014

- SANTOS, Hugo Luz dos, "*Plaidoyer por uma 'distribuição dinâmica do ónus da prova' e pela 'teoria das esferas de risco' à luz do recente acórdão do Supremo Tribunal de Justiça, de 18/12/2013: o (admirável) 'novo mundo' no Homebanking?*" in RED -Revista Eletrónica de Direito, n.o 1, Fev. 2015, CIJE/FDUP <www.cije.up.pt/revistared> (20.04.2015);

- SANTOS, Verónica, "*As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de phishing e pharming. A questão da responsabilidade no âmbito das operações bancárias não autorizadas*." Dissertação de Mestrado, Faculdade de Direito da Universidade Católica Portuguesa de Lisboa, 2018;

- SILVA, João Calvão, "*Serviços de pagamento e responsabilidade civil*", in: Estudos em homenagem a Rui Manchete, Almedina, 2015, p. 339-376

- TRELEAVEN, Philip, *Financial regulation of FinTech*, Journal of Financial Perspectives, Vol. 3, No. 3, 2015

- UNITED NATIONS ENVIRONMENT PROGRAMME, *Fintech and sustainable development. Assessing the implications*, dezembro 2016, disponível em http://unepinquiry.org/wpcontent/uploads/2016/12/Fintech_and_Sustainable_Developent_Assessing_the_Implications.pdf

- VALE, Sebastião Barros, *PDS2, GDPR and Banking Secrecy: what role for consent?*,

- VAZ, Ana Sofia Lopes, *O acesso a informações bancárias e financeiras por parte da Autoridade Tributária e Aduaneira. O fim do sigilo bancário?*, Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto, 2017

- ZACHARIADIS, Markos, *The API Economy and Digital Transformation in Financial Services: The Case of Open Banking*, SWIFT Institute Working Paper No. 2016-001, 2017

- ZUNZUNEGUI, Fernando, *Digitalisation of payment services*, Ibero-American Institute for Law and Finance Working Paper No. 5/2018, 2018

ÍNDICE JURISPRUDENCIAL